Strongly Universal Quantum Turing Machines and Invariance of Kolmogorov Complexity

Markus Müller

***Abstract*— We show that there exists a universal quantum Turing machine (UQTM) that can simulate every other QTM *until the other QTM has halted* and then halt itself with probability one. This extends work by Bernstein and Vazirani who have shown that there is a UQTM that can simulate every other QTM for an arbitrary, but preassigned number of time steps.**

As a corollary to this result, we give a rigorous proof that quantum Kolmogorov complexity as defined by Berthiaume et. al. is invariant, i.e. depends on the choice of the UQTM only up to an additive constant.

Our proof is based on a new mathematical framework for QTMs, including a thorough analysis of their halting behaviour. We introduce the notion of mutually orthogonal halting spaces and show that the information encoded in an input qubit string can always be effectively decomposed into a classical and a quantum part.

***Index Terms*— Quantum Turing Machine, Kolmogorov Complexity, Universal Quantum Computer, Quantum Kolmogorov Complexity, Halting Problem.**

I. INTRODUCTION

SINCE the classical Turing machine turned out to be so useful as a formal model for computation, much work has been done to generalize it to quantum computation. In 1985, D. Deutsch [1] proposed the first model of a quantum Turing machine (QTM), elaborating on an even earlier idea by Feynman [2]. Bernstein and Vazirani [3] worked out the theory in more detail and proved that there exists an efficient universal QTM (it will be discussed below in what sense). A more compact presentation of these results can be found in the book by J. Gruska [4]. Ozawa and Nishumura [5] gave necessary and sufficient conditions that a QTM's transition function results in unitary time evolution. Benioff [6] has worked out a slightly different definition which is based on a local Hamiltonian instead of a local transition amplitude.

A. Quantum Turing Machines and their Halting Conditions

Our discussion will rely on the definition by Bernstein and Vazirani. We will describe their model in detail in Subsection II-B. Similarly to a classical TM[1], a QTM consists of an infinite tape, a control, and a single tape head that moves along the tape cells. The QTM as a whole evolves unitarily in discrete time steps. The (global) unitary time evolution U is completely determined by a local transition amplitude δ which only affects the single tape cell where the head is pointing to.

There has been a lengthy discussion in the literature on the question when we can consider a QTM as having *halted* on some input and how this is compatible with unitary time evolution, see e.g. [7], [8], [9], [10], [11]. We will not get into this discussion, but rather analyze in detail the simple definition for halting by Bernstein and Vazirani, which will turn out to be useful and correct (and unique) in many respects.

Suppose a QTM M runs on some input $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$ for t time steps. The control of M will then be in some state (obtained by partial trace over all the other parts of the QTM) which we denote $M^t_{\mathbf{C}}(|\psi\rangle)$ (the letter $\mathbf{C}$ stands for "control"). In general, this is some mixed state on the finite-dimensional Hilbert space $\mathcal{H}_{\mathbf{C}}$ that describes the control. By definition of a QTM (see Subsection II-B), there is a specified *final state* $|q_f\rangle \in \mathcal{H}_{\mathbf{C}}$. According to [3], we say that the QTM M halts at time T on input $|\psi\rangle$ if

$$\langle q_f|M^T_{\mathbf{C}}(|\psi\rangle)|q_f\rangle = 1 \text{ and } \langle q_f|M^t_{\mathbf{C}}(|\psi\rangle)|q_f\rangle = 0 \quad \forall t < T.$$

We can rephrase this definition as $M^T_{\mathbf{C}}(|\psi\rangle) = |q_f\rangle\langle q_f|$, i.e. the control is *exactly* in the final state at time T, and $\operatorname{supp}\left(M^t_{\mathbf{C}}(|\psi\rangle)\right) \subset |q_f\rangle^\perp$, i.e. the control state is exactly orthogonal to the halting state at any time $t < T$ before the halting time.

For most inputs $|\psi\rangle$, there will be no time $T \in \mathbb{N}$ such that both conditions above are satisfied. Let us call such inputs $|\psi\rangle$ *non-halting*. Nevertheless, there are many inputs that satisfy these conditions (call them T*-halting* with $T \in \mathbb{N}$ as given above), for example some classical inputs that make M behave like a classical TM. Moreover, most well-known quantum algorithms (e.g. the quantum Fourier transform) that work by application of a fixed number of unitary gates can be translated into an algorithm for a QTM, consisting of a classical subroutine that controls the application of the unitary transformations as well as the halting behaviour. Thus, all the important quantum algorithms known so far will satisfy the conditions above if they are correctly implemented on a QTM.

Moreover, these halting conditions are very useful. Given two QTMs M_1 and M_2, they enable one to construct a QTM M which carries out the computations of M_1, *followed by the computations of* M_2, just by redirecting the final state $|q_f\rangle$ of M_1 to the starting state $|q_0\rangle$ of M_2 (see [3, Dovetailing Lemma 4.2.6]). In addition, they allow for a simple proof that QTMs are *quantum operations*, which itself can be used to prove certain properties of QTMs as we have shown in [12]. Even more important, at each single time step, an outside observer can make a measurement of the control state, described by the operators $|q_f\rangle\langle q_f|$ and $\mathbf{1} - |q_f\rangle\langle q_f|$ (thus observing the halting time), without spoiling the computation, as long as the input $|\psi\rangle$ is halting. As soon as halting is detected, the observer can

M. Müller is with the Institute of Mathematics, Technical University of Berlin (e-mail: mueller@math.tu-berlin.de).

[1] We use the terms "Turing machine" (TM) and "computer" synonymously for "partial recursive function from $\{0,1\}^*$ to $\{0,1\}^*$", where $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$ denotes the finite binary strings.

extract the output quantum state from the output track (tape) and use it for further quantum information processing.[2]

Another reason to cling to the forementioned halting condition comes from the intention to define *quantum Kolmogorov complexity*. It is instructive to look at some aspects of classical Kolmogorov complexity, since it shares many properties with its quantum counterpart. The Kolmogorov complexity of a finite bit string is the minimal length of a computer program that, fed into a universal TM, outputs the string. While this quantity has many interesting applications (see [13]), it is indispensable for its definition to consider certain computer programs that have astronomically large halting times. For example, there is a short computer program that calculates the string s consisting of N zeroes, where $N = 10^{10^{10^{\cdots}}}$ is a power tower of 1000 tens, meaning that the complexity of s is small, although s is astronomically long. While such programs can never be executed in practice, one has to consider them nevertheless in dealing with Kolmogorov complexity.

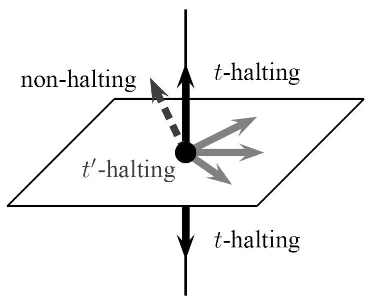

Fig. 1. Mutually Orthogonal Halting Spaces

For quantum complexity, the situation will obviously be similar: There will be certain computations with huge halting times that have to be considered in principle. This explains why it is *not* a good idea to allow a certain small error in the halting conditions. Replacing the forementioned conditions by $|\langle q_f | M_{\mathbf{C}}^t(|\psi\rangle)|q_f\rangle - \delta_{tT}| \leq \varepsilon$ for some small $\varepsilon > 0$, for example, means that there is only a small perturbation if an outside observer measures the halting state of the control. The problem is that the halting time T is not known in advance and can be *huge*. Thus, if the observer measures periodically (or even at some predefined sequence of times like $t_1 = 1$, $t_2 = 10$, $t_3 = 100$ and so on), the small errors will add up and disturb the computation substantially before it is finished.

In Subsection III-A, we analyze the resulting halting structure of input vectors. We show that inputs $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$ with some fixed length $n \in \mathbb{N}_0$ that make the QTM M halt after $t \in \mathbb{N}$ steps form a linear subspace $\mathcal{H}_M^{(n)}(t) \subset \left(\mathbb{C}^2\right)^{\otimes n}$. Moreover, inputs with different halting times are mutually orthogonal, i.e. $\mathcal{H}_M^{(n)}(t) \perp \mathcal{H}_M^{(n)}(t')$ if $t \neq t'$. According to the halting conditions given above, this is almost obvious: Superpositions of t-halting inputs are again t-halting, and inputs with different halting times can be perfectly distinguished, just by observing their halting time. In Figure 1, a geometrical picture of the halting space structure is shown: The whole space $\mathbb{R}^3$ represents the space of inputs of some fixed length n, i.e. $\left(\mathbb{C}^2\right)^{\otimes n}$, while the plane and the straight line represent two different halting spaces $\mathcal{H}_M^{(n)}(t')$ and $\mathcal{H}_M^{(n)}(t)$. Every vector within these subspaces is perfectly halting, while every vector "in between" is non-halting and not considered a useful input for the QTM M. One might suspect that one looses a lot by throwing away every not perfectly halting input, but based on the calculations in Section III, we formulate a conjecture (Conjecture 3.15) which states that for every almost halting input, there is some perfectly halting input that almost gives the same output.

[2]Note that this halting protocol is easily shown to be equivalent to that by Ozawa [9]; formally, the latter can be constructed by adding an ancilla system to the QTM which carries the output state from the moment of halting on.

B. Different Notions of Universality for QTMs

Bernstein and Vazirani [3] have shown that there exists a universal QTM (UQTM) $\mathcal{U}$. It is important to understand what exactly they mean by "universal". According to [3, Thm. 7.0.2], this UQTM $\mathcal{U}$ has the property that for every QTM M there is some classical bit string $s_M \in \{0,1\}^*$ (containing a description of the QTM M) such that

$$\left\| \mathcal{U}(s_M, T, \delta, |\psi\rangle) - M_{\mathbf{O}}^T(|\psi\rangle) \right\|_{\mathrm{Tr}} < \delta \qquad (1)$$

for every input $|\psi\rangle$, accuracy $\delta > 0$ and number of time steps $T \in \mathbb{N}$. Here, $\|\cdot\|_{\mathrm{Tr}}$ is the trace distance, and $M_{\mathbf{O}}^T(|\psi\rangle)$ is the content of the output tape of M after T steps of computation (the notation will be defined exactly in Subsection II-B).

This means that the UQTM $\mathcal{U}$ simulates every other QTM M within any desired accuracy (and outputs an approximate description of the output of M and halts), as long as the number of time steps T is given as input in advance. Moreover, Bernstein and Vazirani have shown that the simulation is *efficient*, i.e. $\mathcal{U}$ takes only polynomially (in T and $1/\delta$) more time steps than M. This is the important point in their paper: They are interested in the *computational complexity* of QTMs, i.e. they want to find evidence that QTMs are more powerful ("faster") than classical TMs. By definition, the algorithms they consider (e.g. those in the complexity class BQP) have the property that their running time T (or an upper bound on it) is known *in advance*. Thus, it is no restriction for computational complexity to demand that the UQTM $\mathcal{U}$ is supplied with the running time T as input.

The situation is completely different if one is interested in studying *quantum Kolmogorov complexity* instead. It will be explained in Subsection I-C below that the universality notion (1) is not enough for proving even the most basic result ("invariance") for quantum Kolmogorov complexity. Something more is needed, namely a generalization of (1): can we drop the requirement to supply $\mathcal{U}$ with the running time T as input, i.e. can we find a QTM $\mathfrak{U}$ that simulates every other QTM M within any desired accuracy just *until the other QTM has halted* and then halts itself, without knowing the halting time T in advance? We call the latter property "strong universality".

In this paper, we give a positive answer to this question and show that such a QTM $\mathfrak{U}$ indeed exists (this is the content of Theorem 1.1). Before discussing the proof idea or the consequences, it is important to understand why this is so difficult to prove, and why it does *not* follow immediately from the existence of a QTM $\mathcal{U}$ that satisfies (1), i.e. that is universal in the sense of Bernstein and Vazirani.

A first attempt could be to program the universal QTM $\mathcal{U}$ to simulate the other QTM M, and, after every time step, to check if the simulation of M has halted or not. If it has halted, then $\mathcal{U}$ halts itself and prints out the output of M, otherwise it continues.

Of course, this works for classical TMs, but for QTMs, there is one problem: In general, the UQTM $\mathcal{U}$ can simulate M only approximately. The reason is the same as for the circuit model, i.e. the set of basic unitary transformations that $\mathcal{U}$ can apply on its tape may be algebraically independent from that of M, making a perfect simulation in principle impossible. But if the simulation is only approximate, then the halting behaviour of M will also be simulated only approximately, which will force $\mathcal{U}$ to halt only approximately. Thus, the restrictive halting conditions given above in Subsection I-A will inevitably be violated, and the computation of $\mathcal{U}$ will be treated as invalid and be thrown away by definition.

This is a severe problem that cannot be circumvented easily. Many ideas for simple solutions must fail, for example the idea to let $\mathcal{U}$ compute an upper bound on the halting time T of all inputs for M of some length n and just to proceed for T time steps: upper bounds on haltings times are incomputable. Another idea is that the computation of $\mathcal{U}$ should somehow consist of a classical part that controls the computation and a quantum part that does the unitary transformations on the data. But this idea is difficult to formalize. Even for classical TMs, there is no general way to split the computation into ”program” and ”data” except for special cases, and for QTMs, by definition, global unitary time evolution can entangle every part of a QTM with every other part.

Our proof idea rests instead on the observation that any *input* for a QTM which is halting (as defined above in Subsection I-A) can be decomposed into a classical and a quantum part, which is related to the mutual orthogonality of the halting spaces, see Subsection I-E for details.

C. Q-Kolmogorov Complexity and its Supposed Invariance

The classical Kolmogorov complexity $C_U(s)$ of a finite bit string $s \in \{0,1\}^*$ is defined as the minimal length of any computer program p that, given as input into a TM M, outputs the string and makes M halt:

$$C_M(s) := \min \{\ell(p) \mid M(p) = s\} \; .$$

For this quantity, running times are not important; all that matters is the input length. There is a crucial result that is the basis for the whole theory of Kolmogorov complexity (see [13]). Basically, it states that the choice of the computer M is not important as long as M is universal; choosing a different universal computer will alter the complexity only up to some additive constant. More specifically, there exists a universal computer U such that for every computer M there is a constant $c_M \in \mathbb{N}$ such that

$$C_U(s) \leq C_M(s) + c_M \qquad \text{for every } s \in \{0,1\}^* \; . \qquad (2)$$

This so-called ”invariance property” follows easily from the existence of a universal computer U in the following sense: There exists a computer U such that for every computer M and every input $s \in \{0,1\}^*$ there is an input $\tilde{s} \in \{0,1\}^*$ such that $U(\tilde{s}) = M(s)$ and $\ell(\tilde{s}) \leq \ell(s) + c_M$, where $c_M \in \mathbb{N}$ is a constant depending only on M. In short, there is a computer U that produces every output that is produced by any other computer, while the length of the corresponding input blows up only by a constant summand. One can think of the bit string $\tilde{s}$ as consisting of the original bit string s and of a description of the computer M (of length c_M).

The quantum generalization of Kolmogorov complexity that we consider in this paper has been first defined by Berthiaume, van Dam and Laplante [14]. Basically, they define the quantum Kolmogorov complexity QC of a string of qubits $|\psi\rangle$ as the length of the shortest string of qubits that, when given as input to a QTM M, makes M output $|\psi\rangle$ and halt. (We give a formal definition of a ”qubit string” in Subsection II-A and of quantum Kolmogorov complexity QC in Subsection II-C).[3] A closely related quantity has been considered recently by Rogers and Vedral [17].

In both cases [14] and [17], it is claimed that quantum Kolmogorov complexity QC is invariant up to an additive constant similar to (2). Nevertheless, in [17] no proof is given and the proof in [14] is incomplete: In that proof, it is stated that the existence of a universal QTM $\mathcal{U}$ in the sense of Bernstein and Vazirani (see Equation (1)) makes it possible to mimic the classical proof and to conclude that the UQTM $\mathcal{U}$ outputs all that every other QTM outputs, implying invariance of quantum Kolmogorov complexity.

But as explained above in Subsection I-B, this conclusion cannot be drawn so easily. Since $\mathcal{U}$ can simulate other QTMs only approximately, it will also simulate their halting behaviour only approximately and thus violate the halting conditions explained in Subsection I-A. To summarize, if there is a short input $|\varphi\rangle$ for a QTM M such that $M(|\varphi\rangle) = |\psi\rangle$, it does not follow from the universality notion (1) that there is some input $|\tilde{\varphi}\rangle$ for $\mathcal{U}$ such that $\mathcal{U}(|\tilde{\varphi}\rangle) \approx |\psi\rangle$ and $\ell(|\tilde{\varphi}\rangle) \leq \ell(|\varphi\rangle) + c_M$ for some constant c_M. Thus, invariance of quantum Kolmogorov complexity does *not* follow from the existence of a universal QTM in the sense of (1), and the proof in [14] is incomplete.

Instead of (1), a stronger notion of universality is needed, namely a ”strongly universal” QTM $\mathfrak{U}$ that, as explained above in Subsection I-B, simulates every other QTM M *until the other QTM has halted* and then halts itself with perfect fidelity, as required by the halting conditions given in Subsection I-A. Then, the classical proof outlined above can be carried over to the quantum situation. In this paper, we prove that such a QTM $\mathfrak{U}$ really exists (Theorem 1.1), and as a corollary, the invariance property for quantum Kolmogorov complexity follows (Theorem 1.2).

[3]While this complexity notion $QC(|\psi\rangle)$ counts the shortest length of a *quantum description* of $|\psi\rangle$, Vitányi [15] and Gács [16] have worked out different definitions for quantum Kolmogorov complexity based on *classical descriptions*. They are not considered in this paper since they do not share the difficulties mentioned above.

D. Main Theorems

One main result of this paper is the existence of a strongly universal QTM that simulates every other QTM until the other QTM has halted and then halts itself. Note that the halting state is attained by $\mathfrak{U}$ *exactly* (with probability one) in accordance with the strict halting conditions given in Subsection I-A.

Theorem 1.1 (Strongly Universal Q-Turing Machine): There is a fixed-length quantum Turing machine $\mathfrak{U}$ such that for every QTM M and every qubit string σ for which $M(\sigma)$ is defined, there is a qubit string σ_M such that

$$\|\mathfrak{U}\left(\sigma_M,\delta\right)-M(\sigma)\|_{\mathrm{Tr}}<\delta$$

for every $\delta\in\mathbb{Q}^+$, where the length of σ_M is bounded by $\ell(\sigma_M)\leq\ell(\sigma)+c_M$, and $c_M\in\mathbb{N}$ is a constant depending only on M.

We conclude from this theorem and a two-parameter generalization given in Proposition 3.14 that quantum Kolmogorov complexity as defined in [14] is indeed invariant, i.e. depends on the choice of the strongly universal QTM only up to some constant:

Theorem 1.2 (Invariance of Q-Kolmogorov Complexity): There is a fixed-length quantum Turing machine $\mathfrak{U}$ such that for every QTM M there is a constant $c_M\in\mathbb{N}$ such that

$$QC_{\mathfrak{U}}^{\searrow 0}(\rho)\leq QC_M^{\searrow 0}(\rho)+c_M\qquad\text{for every qubit string }\rho.$$

Moreover, for every QTM M and every $\delta,\Delta\in\mathbb{Q}^+$ with $\delta<\Delta$, there is a constant $c_{M,\delta,\Delta}\in\mathbb{N}$ such that

$$QC_{\mathfrak{U}}^{\Delta}(\rho)\leq QC_M^{\delta}(\rho)+c_{M,\delta,\Delta}\qquad\text{for every qubit string }\rho.$$

All the proofs are given in Section III, while the ideas of the proofs are outlined in the next subsection.

E. Ideas of Proof

The proof of Theorem 1.1 relies on the observation about the mutual orthogonality of the halting spaces, as explained in Subsection I-A. Fix some QTM M, and denote the set of vectors $|\psi\rangle\in\left(\mathbb{C}^2\right)^{\otimes n}$ which cause M to halt at time t by $\mathcal{H}_M^{(n)}(t)$. If $|\varphi\rangle\in\left(\mathbb{C}^2\right)^{\otimes n}$ is any halting input for M, then we can decompose $|\varphi\rangle$ in some sense into a classical and a quantum part. Namely, the information contained in $|\varphi\rangle$ can be split into a

- classical part: The vector $|\varphi\rangle$ is an element of *which* of the subspaces $\mathcal{H}_M^{(n)}(t)$?
- quantum part: Given the halting time τ of $|\varphi\rangle$, then *where* in the corresponding subspace $\mathcal{H}_M^{(n)}(\tau)$ is $|\varphi\rangle$ situated?

Our goal is to find a QTM $\mathfrak{U}$ and an encoding $|\tilde\varphi\rangle\in\left(\mathbb{C}^2\right)^{\otimes(n+1)}$ of $|\varphi\rangle$ which is only one qubit longer and which makes the (cleverly programmed) QTM $\mathfrak{U}$ output a good approximation of $M(|\varphi\rangle)$. First, we extract the quantum part out of $|\varphi\rangle$. While $\dim\left(\mathbb{C}^2\right)^{\otimes n}=2^n$, the halting space $\mathcal{H}_M^{(n)}(\tau)$ that contains $|\varphi\rangle$ is only a subspace and might have much smaller dimension $d<2^n$. This means that we need less than n qubits to describe the state $|\varphi\rangle$; indeed, $\lceil\log_2 d\rceil$ qubits are sufficient. In other words, there is some kind of ”standard compression map” $\mathcal{C}$ that maps every vector $|\psi\rangle\in\mathcal{H}_M^{(n)}(\tau)$ into the $\lceil\log_2 d\rceil$-qubit-space $\left(\mathbb{C}^2\right)^{\otimes\lceil\log_2 d\rceil}$. Thus, the qubit string $\mathcal{C}|\varphi\rangle$ of length $\lceil\log_2 d\rceil\leq n$ can be considered as the ”quantum part” of $|\varphi\rangle$.

So how can the classical part of $|\varphi\rangle$ be encoded into a short classical binary string? Our task is to specify what halting space $\mathcal{H}_M^{(n)}(\tau)$ corresponds to $|\varphi\rangle$. Unfortunately, it is not possible to encode the halting time τ directly, since τ might be huge and may not have a short description. Instead, we can encode the *halting number*. Define the halting time sequence $\{t_i\}_{i=1}^N$ as the set of all integers $t\in\mathbb{N}$ such that $\dim\mathcal{H}_M^{(n)}(t)\geq 1$, ordered such that $t_i<t_{i+1}$ for every i, that is, the set of all halting times that can occur on inputs of length n. Thus, there must be some $i\in\mathbb{N}$ such that $\tau=t_i$, and i can be called the halting number of $|\varphi\rangle$. Now, we assign code words c_i to the halting numbers i, that is, we construct a prefix code $\{c_i\}_{i=1}^N\subset\{0,1\}^*$. We want the code words to be short; we claim that we can always choose the lengths as

$$\ell(c_i)=n+1-\lceil\log_2\dim\mathcal{H}_M^{(n)}(t_i)\rceil\ .$$

This can be verified by checking the Kraft inequality:

$$\begin{aligned}\sum_{i=1}^N 2^{-\ell(c_i)} &= 2^{-n}\sum_{i=1}^N 2^{\lceil\log_2\dim\mathcal{H}_M^{(n)}(t_i)\rceil-1}\\ &\leq 2^{-n}\sum_{i=1}^n\dim\mathcal{H}_M^{(n)}(t_i)\leq 2^{-n}\dim\left(\mathbb{C}^2\right)^{\otimes n}\\ &\leq 1,\end{aligned}$$

since the halting spaces are mutually orthogonal.

Putting classical and quantum part of $|\varphi\rangle$ together, we get

$$|\tilde\varphi\rangle:=c_i\otimes\mathcal{C}|\varphi\rangle\ ,$$

where i is the halting number of $|\varphi\rangle$. Thus, the length of $|\tilde\varphi\rangle$ is exactly $n+1$.

Let s_M be a self-delimiting description of the QTM M. The idea is to construct a QTM $\mathfrak{U}$ that, on input $s_M\otimes|\tilde\varphi\rangle$, proceeds as follows:

- By *classical* simulation of M, it computes descriptions of the halting spaces $\mathcal{H}_M^{(n)}(1),\mathcal{H}_M^{(n)}(2),\mathcal{H}_M^{(n)}(3),\ldots$ and the corresponding code words $c_1,c_2,c_3,\ldots$ one after the other, until at step τ, it finds the code word c_i that equals the code word in the input.
- Afterwards, it applies a (quantum) decompression map to approximately reconstruct $|\varphi\rangle$ from $\mathcal{C}|\varphi\rangle$.
- Finally, it simulates (quantum) for τ time steps the time evolution of M on input $|\varphi\rangle$ and then halts, whatever happens with the simulation.

Such a QTM $\mathfrak{U}$ will have the strong universality property as stated in Theorem 1.1. Unfortunately, there are many difficulties that have to be overcome by the proof in Section III:

- Also classically, QTMs can only be simulated approximately. Thus, it is for example impossible for $\mathfrak{U}$ to decide by classical simulation whether the QTM M halts on some input $|\psi\rangle$ perfectly or only approximately at some time t. Thus, we have to define certain δ-approximate halting spaces $\mathcal{H}_M^{(n,\delta)}(t)$ and prove a lot of lemmas with nasty inequalities.
- Since our approach is as general as possible, we have to consider mixed inputs and outputs as well.

- The forementioned prefix code must have the property that one code word can be constructed after the other (since the sequence of all halting times is incomputable), see Lemma 3.12.

We show that all these difficulties (and some more) can be overcome, and the idea outlined above can be converted to a formal proof of Theorem 1.1 and the second part of Theorem 1.2 which we give in full detail in Section III.

Unfortunately, for the first part of Theorem 1.2, concerning the complexity notion $QC^{\searrow 0}$, a more general result is needed which is stated in Proposition 3.14, since this complexity notion needs an additional parameter as input. For this proposition, the proof idea outlined above does not work, but needs to be modified. The idea for the modified proof of that proposition is to make the QTM $\mathfrak{U}$ determine the halting number of the input (and thus the halting time) directly by projective measurement in the basis of (approximations of) the halting spaces. We will not prove Proposition 3.14 in full detail, but only sketch the proof idea there, since the technical details are similar to that of the proof of Theorem 1.1.

II. Mathematical Framework and Formalism

Here, we introduce the formalism that is used in Section III to describe qubit strings, quantum Turing machines and quantum Kolmogorov complexity. We denote the density operators on a Hilbert space $\mathcal{H}$ by $\mathcal{T}_1^+(\mathcal{H})$ (i.e. the positive trace-class operators with trace 1).

A. Variable-length Qubit Strings

Let $\mathcal{H}_k := \left(\mathbb{C}^{\{0,1\}}\right)^{\otimes k}$ be the Hilbert space of k qubits ($k \in \mathbb{N}_0$). We write $\mathbb{C}^{\{0,1\}}$ for $\mathbb{C}^2$ to indicate that we fix two orthonormal *computational basis vectors* $|0\rangle$ and $|1\rangle$. Since we want to allow superpositions of different lengths k, we consider the Hilbert space $\mathcal{H}_{\{0,1\}^*}$ defined as

$$\mathcal{H}_{\{0,1\}^*} := \bigoplus_{k=0}^{\infty} \mathcal{H}_k \ .$$

The classical finite binary strings $\{0,1\}^*$ are identified with the computational basis vectors in $\mathcal{H}_{\{0,1\}^*}$, i.e. $\mathcal{H}_{\{0,1\}^*} \simeq \ell^2(\{\lambda, 0, 1, 00, 01, \ldots\})$, where λ denotes the empty string. We also use the notation

$$\mathcal{H}_{\leq n} := \bigoplus_{k=0}^{n} \mathcal{H}_k$$

and treat it as a subspace of $\mathcal{H}_{\{0,1\}^*}$. A (variable-length) *qubit string* σ is a density operator on $\mathcal{H}_{\{0,1\}^*}$. We define the *length* $\ell(\sigma) \in \mathbb{N}_0 \cup \{\infty\}$ of a qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ as

$$\ell(\sigma) := \min\{n \in \mathbb{N}_0 \ | \ \sigma \in \mathcal{T}_1^+(\mathcal{H}_{\leq n})\} \tag{3}$$

or as $\ell(\sigma) = \infty$ if this set is empty (this case will not be considered in the following). This means for example that the density operator $\sigma := \frac{1}{\sqrt{2}}(|0\rangle + |11\rangle) \times c.c.$ is a (pure) qubit string of length $\ell(\sigma) = 2$, i.e. the length of a variable-length qubit string equals the maximal length of any computational basis vector that has non-zero coefficient in the superposition. This is motivated by the fact that the state σ needs at least $\ell(\sigma)$ cells on a QTM's tape to be stored perfectly (compare Subsection II-B). An alternative approach would be to consider the expectation value $\bar{\ell}$ of the length instead, which has been proposed by Rogers and Vedral [17], see also the discussion in Section IV.

There are two reasons for considering variable-length and also mixed qubit strings. First, we want our result to be as general as possible. Second, a QTM will naturally produce superpositions of qubit strings of different lengths; mixed outputs appear naturally while tracing out the other parts of the QTM (input track, control, head) after halting.

In contrast to the classical situation, there are uncountably many qubit strings that cannot be perfectly distinguished by means of any quantum measurement. Thus, since QTMs are discrete machines, one cannot expect in general that qubit strings are computed exactly, but one has to allow a certain error tolerance. A good measure for the ability to distinguish between two quantum states is the trace distance (cf. [18])

$$\|\rho - \sigma\|_{\mathrm{Tr}} := \frac{1}{2}\mathrm{Tr}\,|\rho - \sigma| = \frac{1}{2}\sum_i |\lambda_i| \ , \tag{4}$$

where the λ_i are the eigenvalues of the Hermitian operator $|\rho - \sigma| := \sqrt{(\rho-\sigma)^*(\rho-\sigma)}$. This distance measure on the qubit strings will be used in our definition of quantum Kolmogorov complexity in Subsection II-C.

B. Mathematical Description of Quantum Turing Machines

Bernstein and Vazirani ([3], Def. 3.2.2) define a quantum Turing machine M as a triplet (Σ, Q, δ), where Σ is a finite alphabet with an identified blank symbol $\#$, and Q is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$. The function $\delta : Q \times \Sigma \to \tilde{\mathbb{C}}^{\Sigma \times Q \times \{L,R\}}$ is called the *quantum transition function*. The symbol $\tilde{\mathbb{C}}$ denotes the set of complex numbers $\alpha \in \mathbb{C}$ such that there is a deterministic algorithm that computes the real and imaginary parts of α to within 2^{-n} in time polynomial in n.

One can think of a QTM as consisting of a two-way infinite tape $\mathbf{T}$ of cells indexed by $\mathbb{Z}$, a control $\mathbf{C}$, and a single "read/write" head $\mathbf{H}$ that moves along the tape. A QTM evolves in discrete, integer time steps, where at every step, only a finite number of tape cells is non-blank. For every QTM, there is a corresponding Hilbert space $\mathcal{H}_{QTM} = \mathcal{H}_{\mathbf{C}} \otimes \mathcal{H}_{\mathbf{T}} \otimes \mathcal{H}_{\mathbf{H}}$, where $\mathcal{H}_{\mathbf{C}} = \mathbb{C}^Q$ is a finite-dimensional Hilbert space spanned by the (orthonormal) control states $q \in Q$, while $\mathcal{H}_{\mathbf{T}} = \ell^2(T)$ and $\mathcal{H}_{\mathbf{H}} = \ell^2(\mathbb{Z})$ are separable Hilbert spaces describing the contents of the tape and the position of the head, where $T = \left\{(x_i)_{i\in\mathbb{Z}} \in \Sigma^{\mathbb{Z}} \mid x_i \neq \# \text{ for finitely many } i \in \mathbb{Z}\right\}$ denotes the set of classical tape configurations with finitely many non-blank symbols.

For our purpose, it is useful to consider a special class of QTMs with the property that their tape $\mathbf{T}$ consists of two different tracks (cf. [3, Def. 3.5.5]), an *input track* $\mathbf{I}$ and an *output track* $\mathbf{O}$. This can be achieved by having an alphabet which is a Cartesian product of two alphabets, in our case $\Sigma = \{0,1,\#\} \times \{0,1,\#\}$. Then, the tape Hilbert space $\mathcal{H}_{\mathbf{T}}$ can be written as $\mathcal{H}_{\mathbf{T}} = \mathcal{H}_{\mathbf{I}} \otimes \mathcal{H}_{\mathbf{O}}$.

The transition function δ generates a linear operator U_M on $\mathcal{H}_{QTM}$ describing the time evolution of the QTM M. We identify $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with the initial state of M on input σ, which is according to the definition in [3] a state on $\mathcal{H}_{QTM}$ where σ is written on the input track over the cell interval $[0, \ell(\sigma)-1]$, the empty state $\#$ is written on the remaining cells of the input track and on the whole output track, the control is in the initial state q_0 and the head is in position 0. By linearity, this e.g. means that the vector $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |11\rangle)$ is identified with the vector $\frac{1}{\sqrt{2}}(|0\#\rangle + |11\rangle)$ on input track cells number 0 and 1.

The global state $M^t(\sigma) \in \mathcal{T}_1^+(\mathcal{H}_{QTM})$ of M on input σ at time $t \in \mathbb{N}_0$ is given by $M^t(\sigma) = (U_M)^t \, \sigma \, (U_M^*)^t$. The state of the control at time t is thus given by partial trace over all the other parts of the machine, that is $M^t_{\mathbf{C}}(\sigma) := \mathrm{Tr}_{\mathbf{T},\mathbf{H}}\left(M^t(\sigma)\right)$ (similarly for the other parts of the QTM). In accordance with [3, Def. 3.5.1], we say that the QTM M *halts at time* $t \in \mathbb{N}$ *on input* $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$, if and only if

$$\langle q_f | M^t_{\mathbf{C}}(\sigma) | q_f \rangle = 1 \text{ and } \langle q_f | M^{t'}_{\mathbf{C}}(\sigma) | q_f \rangle = 0 \quad \forall t' < t, \quad (5)$$

where $q_f \in Q$ is the final state of the control (specified in the definition of M) signalling the halting of the computation. See Subsection I-A for a detailed discussion of these conditions (5).

We can now interpret a QTM as a partial map from the qubit strings to the qubit strings. Note that this point of view is different from e.g. that of Ozawa [9] who described a QTM as a map from Σ^* to the set of probability distributions on Σ^*. Our point of view is motivated by the definition of the complexity of a qubit string in terms of qubit descriptions as explained below in Subsection II-C.

Definition 2.1 (Quantum Turing Machine (QTM)): A partial map $M : \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}) \to \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ will be called a QTM, if there is a Bernstein-Vazirani two-track QTM $\tilde{M} = (\Sigma, Q, \delta)$ (see [3], Def. 3.5.5) with the following properties:

- $\Sigma = \{0,1,\#\} \times \{0,1,\#\}$,
- the corresponding time evolution operator $U_{\tilde{M}}$ is unitary,
- if $\tilde{M}$ halts on input σ at some time $t \in \mathbb{N}$, then $M(\sigma) = \mathcal{R}\left(\tilde{M}^t_{\mathbf{O}}(\sigma)\right)$; otherwise, $M(\sigma)$ is undefined. Here, the quantum operation $\mathcal{R} : \mathcal{T}_1^+(\mathcal{H}_{\mathbf{O}}) \to \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ denotes the "read out" of the output and is defined as follows:
  - If $(x_i)_{i\in\mathbb{Z}} \in \{0,1,\#\}^{\mathbb{Z}}$ is some classical output track configuration, then $R(x_i) := (x_0, x_1, \ldots, x_{k-1})$, where $k := \min\{n \in \mathbb{N}_0 \mid x_n = \#\}$, i.e. R reads off the first bits starting in position 0 up to the first blank symbol,
  - if $|\psi\rangle \in \mathcal{H}_{\mathbf{O}}$ and $|\psi\rangle = \sum_{t\in\{0,1,\#\}^{\mathbb{Z}}} \alpha_t |t\rangle$, then $R|\psi\rangle := \sum_{t\in\{0,1,\#\}^{\mathbb{Z}}} \alpha_t |Rt\rangle$,
  - for every $\rho \in \mathcal{T}_1^+(\mathcal{H}_{\mathbf{O}})$, let $\mathcal{R}(\rho) := R\rho R^*$.

A *fixed-length QTM* is the restriction of a QTM to the domain $\bigcup_{n\in\mathbb{N}_0} \mathcal{T}_1^+(\mathcal{H}_n)$ of fixed-length qubit strings.

Note that while the exact choice of the halting conditions (5) is important as explained in Subsection I-A, the results in this paper are insensitive to changing the details of the input and output conventions (e.g. there are different ways to define the way to read the output).

C. Quantum Kolmogorov Complexity

Quantum Kolmogorov complexity has first been defined by Berthiaume, van Dam, and Laplante [14]. They define the complexity $QC(\rho)$ of a qubit string ρ as the length of the shortest qubit string that, given as input into a QTM M, makes M output ρ and halt. Since there are uncountably many qubit strings, but a QTM can only apply a countable number of transformations (analogously to the circuit model), it is necessary to introduce a certain error tolerance $\delta > 0$.

This can be done in essentially two ways: First, one can just fix some tolerance $\delta > 0$. Second, one can demand that the QTM outputs the qubit string ρ as accurately as one wants, by supplying the machine with a second parameter as input that represents the desired accuracy. This is analogous to a classical computer program that computes the number $\pi = 3.14\ldots$: A second parameter $k \in \mathbb{N}$ can make the program output π to k digits of accuracy, for example. We consider both approaches and follow the lines of [14] except for slight technical modifications (e.g. they use the fidelity while we use the trace distance):

Definition 2.2 (Quantum Kolmogorov Complexity): Let M be a QTM and $\rho \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ a variable-length qubit string. For every $\delta > 0$, we define the *finite-error quantum Kolmogorov complexity* $QC_M^\delta(\rho)$ as the minimal length of any qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ such that the corresponding output $M(\sigma)$ has trace distance from ρ smaller than δ,

$$QC_M^\delta(\rho) := \min\left\{\ell(\sigma) \mid \|\rho - M(\sigma)\|_{\mathrm{Tr}} \leq \delta\right\} .$$

Similarly, we define the *approximation-scheme quantum Kolmogorov complexity* $QC_M^{\searrow 0}(\rho)$ as the minimal length of any qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ such that when given M as input together with any integer k, the output $M(\sigma, k)$ has trace distance from ρ smaller than $1/k$:

$$QC_M^{\searrow 0}(\rho) := \min\left\{\ell(\sigma) \,\middle|\, \|\rho - M(\sigma,k)\|_{\mathrm{Tr}} \leq \frac{1}{k} \forall k \in \mathbb{N}\right\} .$$

For the definition of $QC^{\searrow 0}$, we have to fix a map to encode two inputs (a qubit string and an integer) into one qubit string; this is easy, see e.g. [13] for the classical case and [12] for the quantum case. Also, using $f(k) := 1/k$ as accuracy required on input k is not important; any other computable and descreasing function f that tends to zero for $k \to \infty$ such that f^{-1} is also computable will give essentially the same result.

Note that if M is at least able to move input data to the output track, then it holds $QC_M^\delta(\rho) \leq \ell(\rho) + c_M$ with some constant $c_M \in \mathbb{N}$ (and similarly for $QC_M^{\searrow 0}$). In [12], we have shown that for ergodic quantum information sources, emitted states $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$ have a complexity rate $\frac{1}{n} QC_{\mathcal{U}}^{\bullet}(|\psi\rangle)$ that is with asymptotic probability 1 arbitrarily close to the von Neumann entropy rate s of the source. This demonstrates that quantum Kolmogorov complexity is a useful notion, and that it is feasible to prove interesting theorems on it.

While this complexity notion $QC(\rho)$ counts the length of the shortest qubit string that makes a QTM output ρ and halt, there have been different definitions for quantum algorithmic complexity by Vitányi [15] and Gács [16]. Their approaches are based on classical descriptions and universal density matrices respectively and are not considered in this paper since they do not have the invariance problem outlined in Subsection I-C. Note also that Definition 2.2 depends on the definition of the length $\ell(\sigma)$ of a qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$; there is a different approach by Rogers and Vedral [17] that uses the expected (average) length $\bar{\ell}$ instead and results in a different notion of quantum Kolmogorov complexity. Nevertheless, it seems that Theorem 1.2 can be carried over to their notion of complexity as well.

III. Construction of a Strongly Universal QTM

A. Halting Subspaces and their Orthogonality

As already explained in Subsection I-A in the introduction, restricting to pure input qubit strings $|\psi\rangle \in \mathcal{H}_n$ of some fixed length $\ell(|\psi\rangle) = n$, the vectors with equal halting time t form a linear subspace of $\mathcal{H}_n$. Moreover, inputs with different halting times are mutually orthogonal, as depicted in Figure 1. We will now use the formalism for QTMs introduced in Subsection II-B to give a formal proof of these statements. We use the subscripts $\mathbf{C}$, $\mathbf{I}$, $\mathbf{O}$ and $\mathbf{H}$ to indicate to what part of the tensor product Hilbert space a vector belongs.

Definition 3.1 (Halting Qubit Strings): Let $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ be a qubit string and M a quantum Turing machine. Then, σ is called *t-halting (for M)*, if M halts on input σ at time $t \in \mathbb{N}$. We define the *halting set* and *halting subspace*

$$\begin{aligned} H_M^{(n)}(t) &:= \{|\psi\rangle \in \mathcal{H}_n \mid |\psi\rangle\langle\psi| \text{ is } t\text{-halting for } M\}\ , \\ \mathcal{H}_M^{(n)}(t) &:= \{\alpha|\psi\rangle \mid |\psi\rangle \in H_M^{(n)}(t), \alpha \in \mathbb{C}\}\ . \end{aligned}$$

Note that the only difference between $H_M^{(n)}(t)$ and $\mathcal{H}_M^{(n)}(t)$ is that the latter set contains non-normalized vectors. It will be shown below that $\mathcal{H}_M^{(n)}(t)$ is indeed a linear subspace.

Theorem 3.2 (Halting Subspaces): For every QTM M, $n \in \mathbb{N}_0$ and $t \in \mathbb{N}$, the set $\mathcal{H}_M^{(n)}(t)$ is a linear subspace of $\mathcal{H}_n$, and

$$\mathcal{H}_M^{(n)}(t) \perp \mathcal{H}_M^{(n)}(t') \text{ for every } t \neq t'\ .$$

Proof. Let $|\varphi\rangle, |\psi\rangle \in H_M^{(n)}(t)$. The property that $|\varphi\rangle$ is t-halting is equivalent to the statement that there are states $|\Phi_q^{t'}\rangle \in \mathcal{H}_{\mathbf{I}} \otimes \mathcal{H}_{\mathbf{O}} \otimes \mathcal{H}_{\mathbf{H}}$ and coefficients $c_q^{t'} \in \mathbb{C}$ for every $t' \leq t$ and $q \in Q$ such that

$$\begin{aligned} V_M^t\left(|\varphi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle\right) &= |q_f\rangle_{\mathbf{C}} \otimes |\Phi_{q_f}^t\rangle\ , & (6) \\ V_M^{t'}\left(|\varphi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle\right) &= \sum_{q \neq q_f} c_q^{t'} |q\rangle_{\mathbf{C}} \otimes |\Phi_q^{t'}\rangle \quad \forall t' < t, & (7) \end{aligned}$$

where V_M is the unitary time evolution operator for the QTM M as a whole, and $|\Psi_0\rangle = |q_0\rangle_{\mathbf{C}} \otimes |\#\rangle_{\mathbf{O}} \otimes |0\rangle_{\mathbf{H}}$ denotes the initial state of the control, output track and head. Note that $|\Psi_0\rangle$ does not depend on the input qubit string (in this case $|\varphi\rangle$).

An analogous equation holds for $|\psi\rangle$, since it is also t-halting by assumption. Consider a normalized superposition $\alpha|\varphi\rangle + \beta|\psi\rangle \in \mathcal{H}_n$:

$$\begin{aligned} V_M^t\left(\,|\alpha\varphi + \beta\psi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle\,\right) &= \alpha V_M^t |\varphi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle \\ &\quad + \beta V_M^t |\psi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle \\ &= \alpha |q_f\rangle_{\mathbf{C}} \otimes |\Phi_{q_f}^t\rangle + \beta |q_f\rangle_{\mathbf{C}} \otimes |\tilde{\Phi}_{q_f}^t\rangle \\ &= |q_f\rangle_{\mathbf{C}} \otimes \left(\alpha|\Phi_{q_f}^t\rangle + \beta|\tilde{\Phi}_{q_f}^t\rangle\right)\ . \end{aligned}$$

Thus, the superposition also satisfies condition (6), and, by a similar calculation, condition (7). It follows that $\alpha|\varphi\rangle + \beta|\psi\rangle$ must also be t-halting.

Let now $|\varphi\rangle \in H_M^{(n)}(t)$ and $|\psi\rangle \in H_M^{(n)}(t')$ such that $t < t'$. Again by equations (6) and (7), it holds

$$\begin{aligned} \langle\varphi|\psi\rangle &= \left({}_{\mathbf{I}}\langle\varphi| \otimes \langle\Psi_0|\right) \left(V_M^t\right)^* V_M^t \left(|\psi\rangle_{\mathbf{I}} \otimes |\Psi_0\rangle\right) \\ &= \sum_{Q \ni q \neq q_f} c_q^t \underbrace{{}_{\mathbf{C}}\langle q_f|q\rangle_{\mathbf{C}}}_{0} \cdot \langle\Phi_{q_f}^t|\tilde{\Phi}_q^t\rangle = 0\ . \end{aligned}$$

It follows that $\mathcal{H}_M^{(n)}(t) \perp \mathcal{H}_M^{(n)}(t')$. □

The physical interpretation of the preceding theorem is straightforward: By linearity of the time evolution, superpositions of t-halting strings are again t-halting, and strings with different halting times can be perfectly distinguished by observing their halting time.

B. Approximate Halting Spaces

We start by defining the notion of approximate halting:

Definition 3.3 (ε-t-halting Property): A qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ will be called *ε-t-halting for M* for some $t \in \mathbb{N}$, $\varepsilon \geq 0$ and M a QTM, if and only if

$$\langle q_f | M_{\mathbf{C}}^{t'}(\sigma) | q_f \rangle \begin{cases} \leq \varepsilon & \text{for } t' < t\ , \\ \geq 1 - \varepsilon & \text{for } t' = t\ . \end{cases}$$

Let $S_n := \left\{|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \mid \||\psi\rangle\| = 1\right\}$ be the unit sphere in $\left(\mathbb{C}^2\right)^{\otimes n}$, and let $U_\delta(|\varphi\rangle) := \left\{|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \mid \||\psi\rangle - |\varphi\rangle\| < \delta\right\}$ be an open ball. The ball $U_\delta(|\varphi\rangle)$ will be called ε-t-halting for M if there is some $|\psi\rangle \in U_\delta(|\varphi\rangle) \cap S_n$ which is ε-t-halting for M. Moreover, we use the following symbols:

- $\mathrm{dist}(S, |\varphi\rangle) := \inf_{s \in S} \||s\rangle - |\varphi\rangle\|$ for any subset $S \subset \left(\mathbb{C}^2\right)^{\otimes n}$ and $|\varphi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$,
- $\left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n} := \left\{|\varphi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \mid \langle e_k|\varphi\rangle \in \mathbb{Q} + i\mathbb{Q} \quad \forall k\right\}$, where $\{|e_k\rangle\}_{k=1}^{2^n}$ denotes the computational basis vectors of $\left(\mathbb{C}^2\right)^{\otimes n}$,
- $|\varphi^0\rangle := \frac{|\varphi\rangle}{\||\varphi\rangle\|}$ for every vector $|\varphi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n} \setminus \{0\}$.

The set of vectors with rational entries, denoted $\left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$, will in the following be used frequently as inputs or outputs of algorithms. Such vectors can be symbolically added or multiplied with rational scalars without any error. Also, given $|a\rangle, |b\rangle \in \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$, it is an easy task to decide unambiguously which vector has larger norm than the other (one can compare the rational numbers $\||a\rangle\|^2$ and $\||b\rangle\|^2$, for example).

Lemma 3.4 (Algorithm for ε-t-halting-Property of Balls): There exists a (classical) algorithm B which, on input $|\varphi\rangle \in \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$, $\delta, \varepsilon \in \mathbb{Q}^+$, $t \in \mathbb{N}$ and a classical description $s_M \in$

$\{0,1\}^*$ of a fixed-length QTM M, always halts and returns either 0 or 1 under the following constraints:

- If $U_\delta(|\varphi\rangle)$ is not ε-t-halting for M, then the output must be 0.
- If $U_\delta(|\varphi\rangle)$ is $\frac{\varepsilon}{4}$-t-halting for M, then the output must be 1.

Proof. The algorithm B computes a set of vectors $\{|\varphi_k\rangle\}_{k=1}^N \subset \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$ such that for every vector $|\psi\rangle \in U_\delta(|\varphi\rangle) \cap S_n$ there is a $k \in \{1,\ldots,N\}$ such that $\| \,|\varphi_k\rangle - |\psi\rangle\| \leq \frac{3}{64}\,\varepsilon$, and also vice versa (i.e. $\mathrm{dist}\left(U_\delta(|\varphi\rangle) \cap S_n, |\varphi_k\rangle\right) \leq \frac{3}{64}\,\varepsilon$ for every k).

For every $k \in \{1,\ldots,N\}$, the algorithm simulates the QTM M on input $|\varphi_k\rangle$ classically for t time steps and computes an approximation $a(t')$ of the quantity $\langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle$ for every $t' \leq t$, such that

$$\left| a(t') - \langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle \right| < \frac{3}{32}\,\varepsilon \qquad \text{for every } t' \leq t\ .$$

How can this be achieved? Since the number of time steps t is finite, time evolution will be restricted to a finite subspace $\tilde{\mathcal{H}}_{\mathbf{T}} \subset \mathcal{H}_{\mathbf{T}}$ corresponding to a finite number of tape cells, which also restricts the state space of the head (that points on tape cells) to a finite subspace $\tilde{\mathcal{H}}_{\mathbf{H}}$. Thus, it is possible to give a matrix representation of the time evolution operator V_M on $\mathcal{H}_{\mathbf{C}} \otimes \tilde{\mathcal{H}}_{\mathbf{T}} \otimes \tilde{\mathcal{H}}_{\mathbf{H}}$, and the expression given above can be numerically calculated just by matrix multiplication and subsequent numerical computation of the partial trace.

Every $|\varphi_k\rangle$ that satisfies $|a(t') - \delta_{t't}| \leq \frac{5}{8}\,\varepsilon$ for every $t' \leq t$ will be marked as "approximately halting". If there is at least one $|\varphi_k\rangle$ that is approximately halting, B shall halt and output 1, otherwise it shall halt and output 0.

To see that this algorithm works as claimed, suppose that $U_\delta(|\varphi\rangle)$ is not ε-t-halting for M, so for every $|\tilde{\psi}\rangle \in U_\delta(|\varphi\rangle)$ there is some $t' \leq t$ such that $\left|\delta_{t't} - \langle q_f | M_{\mathbf{C}}^{t'}(|\tilde{\psi}\rangle\langle\tilde{\psi}|)|q_f\rangle\right| > \varepsilon$. Also, for every $k \in \{1,\ldots,N\}$, there is some vector $|\psi\rangle \in U_\delta(|\varphi\rangle) \cap S_n$ with $\| \,|\varphi_k\rangle - |\psi\rangle\| \leq \frac{3}{64}\,\varepsilon$, so

$$\begin{aligned}
\Delta_k \quad &:= \quad \left|\delta_{t't} - \langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle\right| \\
&\geq \quad \left|\delta_{t't} - \langle q_f | M_{\mathbf{C}}^{t'}(|\psi\rangle\langle\psi|)|q_f\rangle\right| \\
&- \quad \left|\langle q_f | M_{\mathbf{C}}^{t'}(|\psi\rangle\langle\psi|)|q_f\rangle - \langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k^0\rangle\langle\varphi_k^0|)|q_f\rangle\right| \\
&- \quad \left|\langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle - \langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k^0\rangle\langle\varphi_k^0|)|q_f\rangle\right| \\
&> \quad \varepsilon - \| \,|\psi\rangle\langle\psi| - |\varphi_k^0\rangle\langle\varphi_k^0|\|_{\mathrm{Tr}} - 2\cdot\left|1 - \|\,|\varphi_k\rangle\|^2\right| \\
&\geq \quad \varepsilon - \|\,|\psi\rangle - |\varphi_k^0\rangle\| - 2\left|1 - \|\,|\varphi_k\rangle\|\right|(1 + \|\,|\varphi_k\rangle\|) \\
&\geq \quad \varepsilon - \frac{3}{64}\,\varepsilon - \|\,|\varphi_k\rangle - |\varphi_k^0\rangle\| - 4\cdot\frac{3}{64}\,\varepsilon \geq \frac{23}{32}\varepsilon\ ,
\end{aligned}$$

where we have used Lemma 1.3 and Lemma 1.5. Thus, for every k is holds

$$\begin{aligned}
\left|a(t') - \delta_{t't}\right| \quad &\geq \quad \Delta_k - \left|\langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle - a(t')\right| \\
&> \quad \frac{23}{32}\varepsilon - \frac{3}{32}\,\varepsilon = \frac{5}{8}\varepsilon\ ,
\end{aligned}$$

which makes the algorithm halt and output 0.

On the other hand, suppose that $U_\delta(|\varphi\rangle)$ is $\frac{\varepsilon}{4}$-t-halting for M, i.e. there is some $|\psi\rangle \in U_\delta(|\varphi\rangle) \cap S_n$ which is $\frac{\varepsilon}{4}$-t-halting for M. By construction, there is some k such that $\|\,|\varphi_k\rangle - |\psi\rangle\| \leq \frac{3}{64}\,\varepsilon$. A similar calculation as above yields $\left|\delta_{t't} - \langle q_f | M_{\mathbf{C}}^{t'}(|\varphi_k\rangle\langle\varphi_k|)|q_f\rangle\right| \leq \frac{17}{32}\varepsilon$ for every $t' \leq t$, so $\left|a(t') - \delta_{t't}\right| \leq \frac{17}{32}\varepsilon + \frac{3}{32}\,\varepsilon = \frac{5}{8}\,\varepsilon$, and the algorithm outputs 1. □

Lemma 3.5 (Algorithm I for Interpolating Subspace): There exists a (classical) algorithm I which, on input $M, N \in \mathbb{N}$, $|\tilde{\varphi}_1\rangle, \ldots, |\tilde{\varphi}_M\rangle$, $|\varphi_1\rangle, \ldots, |\varphi_N\rangle \in \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$, $d \in \mathbb{N}$, $\mathbb{Q}^+ \ni \Delta > \delta$ and $\mathbb{Q}^+ \ni \tilde{\Delta} > \tilde{\delta}$, always halts and returns the description of a pair $(i, \tilde{U})$ with $i \in \{0,1\}$ and $\tilde{U} \subset \left(\mathbb{C}^2\right)^{\otimes n}$ a linear subspace, under the following constraints:

- If the output is $(1, \tilde{U})$, then $\tilde{U} \subset \left(\mathbb{C}^2\right)^{\otimes n}$ must be a subspace of dimension $\dim \tilde{U} = d$ such that $\mathrm{dist}(\tilde{U}, |\varphi_k\rangle) < \Delta$ for every k and $\mathrm{dist}(\tilde{U}, |\tilde{\varphi}_l\rangle) > \tilde{\delta}$ for every l.
- If there exists a subspace $U \subset \left(\mathbb{C}^2\right)^{\otimes n}$ of dimension $\dim U = d$ such that $\mathrm{dist}(U, |\varphi_k\rangle) \leq \delta$ for every k and $\mathrm{dist}(U, |\tilde{\varphi}_l\rangle) \geq \tilde{\Delta}$ for every l, then the output must be of the[4] form $(1, \tilde{U})$.

The description of the subspace $\tilde{U}$ is a list of linearly independent vectors $\{|\tilde{u}_i\rangle\}_{i=1}^d \subset \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n} \cap \tilde{U}$.

Proof. Proving this lemma is a routine (but lengthy) excercise. The idea is to construct an algorithm that looks for such a subspace by brute force, that is, by discretizing the set of all subspaces within some (good enough) accuracy. We omit the details. □

We proceed by defining the notion of an *approximate halting space*. Note that the definition depends on the details of the previously defined algorithms in Lemma 3.4 and 3.5 (for example, there are always different possibilities to compute the necessary discretizations). Thus, we fix a concrete instance of all those algorithms for the rest of the paper.

Definition 3.6 (Approximate Halting Spaces): We define[5] the δ-approximate halting space $\mathcal{H}_M^{(n,\delta)}(t) \subset \left(\mathbb{C}^2\right)^{\otimes n}$ and the δ-approximate halting accuracy $\varepsilon_M^{(n,\delta)}(t) \in \mathbb{Q}$ as the outputs of the following classical algorithm on input $n, t \in \mathbb{N}$, $0 < \delta \in \mathbb{Q}$ and $s_M \in \{0,1\}^*$ a classical description of a fixed-length QTM M:

(1) Let $\varepsilon := 18\,\delta$.
(2) Compute a covering of S_n of open balls of radius δ, that is, a set of vectors $\{|\psi_1\rangle, \ldots, |\psi_L\rangle\} \subset \left(\mathbb{C}^2\right)_{\mathbb{Q}}^{\otimes n}$ ($L \in \mathbb{N}$) with $\|\,|\psi_k\rangle\| \in \left(1 - \frac{\delta}{2}, 1 + \frac{\delta}{2}\right)$ for every $k \in \{1,\ldots,L\}$ such that $S_n \subset \bigcup_{i=1}^L U_\delta(|\psi_i\rangle)$.
(3) For every $k \in \{1,\ldots,L\}$, compute $B(|\psi_k\rangle, \delta, \varepsilon, t, s_M)$ and $B(|\psi_k\rangle, \delta, 18\,\delta, t, s_M)$, where B is the algorithm for testing the ε-t-halting property of balls of Lemma 3.4. If the output is 0 for every k, then output $(\{0\}, \varepsilon)$ and halt. Otherwise set for $\mathbb{N}_0 \ni N \leq L$ and $\mathbb{N}_0 \ni K \leq L$

$$\begin{aligned}
\{|\varphi_i\rangle\}_{i=1}^N \quad &:= \quad \{|\psi_k\rangle \ | \ B(|\psi_k\rangle, \delta, \varepsilon, t, s_M) = 1\}\ , \\
\{|\tilde{\varphi}_i\rangle\}_{i=1}^K \quad &:= \quad \{|\psi_k\rangle \ | \ B(|\psi_k\rangle, \delta, 18\,\delta, t, s_M) = 0\}\ .
\end{aligned}$$

If $N = 0$, i.e. if the set $\{|\varphi_i\rangle\}_{i=1}^N$ is empty, output $(\{0\}, \varepsilon)$ and halt.

[4] $\tilde{U}$ will then be an approximation of U.

[5] From a pedantic point of view, the notation should rather read $\mathcal{H}_{s_M}^{(n,\delta)}(t)$ instead of $\mathcal{H}_M^{(n,\delta)}(t)$, since this space depends also on the choice of the classical description s_M of M.

(4) Set $d := 2^n$.
(5) Let $\Delta := 2\delta$, $\tilde\Delta := \frac{7}{4}\delta$ and $\tilde\delta := \frac{3}{2}\delta$. Use the algorithm I of Lemma 3.5 to search for an intersecting subspace, i.e., compute $I(K, N, |\tilde\varphi_1\rangle, \ldots, |\tilde\varphi_K\rangle, |\varphi_1\rangle, \ldots, |\varphi_N\rangle, d, \Delta, \delta, \tilde\Delta, \tilde\delta)$. If the output of I is $(1, \tilde U)$, output $\left(\tilde U, \varepsilon\right)$ and halt.
(6) Set $d := d - 1$. If $d \geq 1$, then go back to step (5).
(7) Set $\varepsilon := \frac{\varepsilon}{2}$ and go back to step (3).

Moreover, let $H_M^{(n,\delta)}(t) := \mathcal{H}_M^{(n,\delta)}(t) \cap S_n$.

Theorem 3.7: The algorithm in Definition 3.6 always terminates on any input; thus, the approximate halting spaces $\mathcal{H}_M^{(n,\delta)}(t)$ are well-defined.

Proof. Define a function $\varepsilon_{min} : S_n \to \mathbb{R}_0^+$ by $\varepsilon_{min}(|\psi\rangle) := \inf\{\varepsilon > 0 \mid |\psi\rangle \text{ is } \varepsilon\text{-}t\text{-halting for } M\}$. Lemma 1.3 and 1.5 yield

$$\left|\varepsilon_{min}(|\psi_1\rangle) - \varepsilon_{min}(|\psi_2\rangle)\right| \leq \|\,|\psi_1\rangle - |\psi_2\rangle\| \;, \qquad (8)$$

so ε_{min} is continuous. For the special case $H_M^{(n)}(t) = \emptyset$, it must thus hold that $\varepsilon_{min}(S_n) := \min_{|\psi\rangle\in S_n} \varepsilon_{min}(|\psi\rangle) > 0$. If the algorithm has run long enough such that $\varepsilon < \varepsilon_{min}(S_n)$, it must then be true that $B(|\psi_k\rangle, \delta, \varepsilon, t, s_M) = 0$ for every $k \in \{1, \ldots, L\}$, since all the balls $U_\delta(|\psi_k\rangle)$ are not ε-t-halting. This makes the algorithm halt in step (3).

Now consider the case $H_M^{(n)}(t) \neq \emptyset$. The continuous function ε_{min} attains a minimum on every compact set $\bar U_\delta(|\psi_k\rangle) \cap S_n$, so let $\varepsilon_k := \min_{|\psi\rangle\in\bar U_\delta(|\psi_k\rangle)\cap S_n} \varepsilon_{min}(|\psi\rangle)$ $(1 \leq k \leq N)$. If $\varepsilon_k = 0$ for every k, then for every k and $\varepsilon > 0$, there is some vector $|\psi\rangle \in U_\delta(|\psi_k\rangle) \cap S_n$ which is ε-t-halting for M, so $B(|\psi_k\rangle, \delta, \varepsilon, t, s_M) = 1$ for every $\varepsilon > 0$, and so $K = 0$ in step (3). Thus, the algorithm I will by construction find the interpolating subspace $\tilde U = \left(\mathbb{C}^2\right)^{\otimes n}$ and cause halting in step (5).

Otherwise, let $\varepsilon_0 := \min\{\varepsilon_k \mid k \in \{1, \ldots, N\}, \varepsilon_k > 0\}$. Suppose that the algorithm has run long enough such that $\varepsilon < \varepsilon_0$. By construction of the algorithm B, if $B(|\psi_k\rangle, \delta, \varepsilon, t, s_M) = 1$, it follows that $U_\delta(|\psi_k\rangle)$ is ε-t-halting for M, but then, $\varepsilon_k \leq \varepsilon < \varepsilon_0$, so $\varepsilon_k = 0$, so there is some $|\psi\rangle \in \bar U_\delta(|\psi_k\rangle) \cap S_n$ which is 0-t-halting for M, so $\mathrm{dist}(\mathcal{H}_M^{(n)}(t), |\psi_k\rangle) \leq \delta$. On the other hand, if $B(|\psi_k\rangle, \delta, 18\,\delta, t, s_M) = 0$, it follows that $U_\delta(|\psi_k\rangle)$ is not $\left(\frac{9}{2}\delta\right)$-$t$-halting for M. Thus, $\mathrm{dist}\left(H_M^{(n)}(t), |\psi_k^0\rangle\right) \geq \frac{9}{2}\delta$ according to (8), so $\mathrm{dist}(\mathcal{H}_M^{(n)}(t) \cap S_n, |\psi_k\rangle) > 4\delta$, and by elementary estimations $\mathrm{dist}(\mathcal{H}_M^{(n)}(t), |\psi_k\rangle) > \frac{7}{4}\delta$. By definition of the algorithm I, it follows that $I(K, N, |\tilde\varphi_1\rangle, \ldots, |\tilde\varphi_K\rangle, |\varphi_1\rangle, \ldots, |\varphi_N\rangle, d, \Delta, \delta, \tilde\Delta, \tilde\delta) = (1, \tilde U)$ for $d := \dim \mathcal{H}_M^{(n)}(t) \geq 1$ and some subspace $\tilde U \subset \left(\mathbb{C}^2\right)^{\otimes n}$, which makes the algorithm halt in step (5). □

Theorem 3.8 (Properties of Approximate Halting Spaces): The approximate halting spaces $\mathcal{H}_M^{(n,\delta)}(t)$ have the following properties:

- *Almost-Halting:* If $|\psi\rangle \in H_M^{(n,\delta)}(t)$, then $|\psi\rangle$ is $(20\,\delta)$-t-halting for M.
- *Approximation:* For every $|\psi\rangle \in H_M^{(n)}(t)$, there is a vector $|\psi^{(\delta)}\rangle \in H_M^{(n,\delta)}(t)$ which satisfies $\|\,|\psi\rangle - |\psi^{(\delta)}\rangle\| < \frac{11}{2}\delta$.
- *Similarity:* If $\delta, \Delta \in \mathbb{Q}^+$ such that $\delta \leq \frac{1}{80}\,\varepsilon_M^{(n,\Delta)}(t)$, then for every $|\psi\rangle \in H_M^{(n,\delta)}(t)$ there is a vector $|\psi^{(\Delta)}\rangle \in H_M^{(n,\Delta)}(t)$ which satisfies $\|\,|\psi\rangle - |\psi^{(\Delta)}\rangle\| < \frac{11}{2}\Delta$.
- *Almost-Orthogonality:* If $|\psi_t\rangle \in H_M^{(n,\delta)}(t)$ and $|\psi_{t'}\rangle \in H_M^{(n,\delta)}(t')$ for $t \neq t'$, then it holds that $|\langle\psi_t|\psi_{t'}\rangle| \leq 4\sqrt{5\delta}$.

Proof. Assume that $H_M^{(n,\delta)}(t) \neq \emptyset$. Let $|\psi\rangle \in H_M^{(n,\delta)}(t) \subset S_n$, and let $\{|\psi_1\rangle, \ldots, |\psi_L\rangle\} \subset \left(\mathbb{C}^2\right)^{\otimes n}$ be the covering of S_n from the algorithm in Definition 3.6. By construction, there is some $k \in \{1, \ldots, K\}$ such that $|\psi\rangle \in U_\delta(|\psi_k\rangle)$. The subspace $\mathcal{H}_M^{(n,\delta)}(t)$ is computed in step (5) of the algorithm in Definition 3.6 via $I(K, N, |\tilde\varphi_1\rangle, \ldots, |\tilde\varphi_K\rangle, |\varphi_1\rangle, \ldots, |\varphi_N\rangle, d, \Delta, \delta, \tilde\Delta, \tilde\delta) = (1, \mathcal{H}_M^{(n,\delta)}(t))$, and since $\mathrm{dist}(\mathcal{H}_M^{(n,\delta)}(t), |\psi_k\rangle) < \delta$, it follows from the properties of the algorithm I in Lemma 3.5 that $|\psi_k\rangle \neq |\tilde\varphi_l\rangle$ for every $l \in \{1, \ldots, K\}$ in step (3) of the algorithm. Thus, $B(|\psi_k\rangle, \delta, 18\,\delta, t, s_M) = 1$, and it follows from the properties of the algorithm B in Lemma 3.4 that $U_\delta(|\psi_k\rangle)$ is $(18\,\delta)$-t-halting for M, so there is some $|\tilde\psi\rangle \in U_\delta(|\psi_k\rangle) \cap S_n$ which is $(18\,\delta)$-t-halting for M. Since $\|\,|\tilde\psi\rangle - |\psi\rangle\| < 2\delta$, the almost-halting property follows from Equation (8).

To prove the approximation property, assume that $H_M^{(n)}(t) \neq \emptyset$. Let $|\psi\rangle \in H_M^{(n)}(t) \subset S_n$; again, there is some $j \in \{1, \ldots, M\}$ such that $|\psi\rangle \in U_\delta(|\psi_j\rangle)$, so $U_\delta(|\psi_j\rangle)$ is 0-t-halting for M, and $B(|\psi_j\rangle, \delta, \varepsilon, t, s_M) = 1$ for every $\varepsilon > 0$ by definition of the algorithm B. For step (3) of the algorithm in Definition 3.6, it thus always holds that $|\psi_j\rangle \in \{|\varphi_i\rangle\}_{i=1}^N$. The output of the algorithm is computed in step (5) via $I(K, N, |\tilde\varphi_1\rangle, \ldots, |\tilde\varphi_K\rangle, |\varphi_1\rangle, \ldots, |\varphi_N\rangle, d, \Delta, \delta, \tilde\Delta, \tilde\delta) = (1, \mathcal{H}_M^{(n,\delta)}(t))$. By definition of I, it holds $\mathrm{dist}(\mathcal{H}_M^{(n,\delta)}(t), |\psi_j\rangle) < \Delta$, and by elementary estimations it follows that $\mathrm{dist}(\mathcal{H}_M^{(n,\delta)}(t) \cap S_n, |\psi_j\rangle) < \frac{\delta}{2} + 2\Delta$, so there is some $|\psi^{(\delta)}\rangle \in H_M^{(n,\delta)}(t)$ such that $\|\,|\psi^{(\delta)}\rangle - |\psi_j\rangle\| < \frac{\delta}{2} + 2\Delta$. Since $\|\,|\psi\rangle - |\psi_j\rangle\| \leq \delta$ and $\Delta = 2\delta$, the approximation property follows.

Notice that under the assumptions given in the statement of the similarity property, it follows from the almost-halting property that if $|\psi\rangle \in H_M^{(n,\delta)}(t)$, then $|\psi\rangle$ must be $\frac{1}{4}\varepsilon_M^{(n,\Delta)}(t)$-$t$-halting for M. Consider the computation of $\mathcal{H}_M^{(n,\Delta)}(t)$ by the algorithm in Definition 3.6. By construction, it always holds that the parameter ε during the computation satisfies $\varepsilon \geq \varepsilon_M^{(n,\Delta)}(t)$, so $|\psi\rangle$ is always $\frac{\varepsilon}{4}$-t-halting for M, and if $|\psi\rangle \in U_\delta(|\psi_j\rangle)$, it follows that $B(|\psi_j\rangle, \delta, \varepsilon, t, s_M) = 1$. The rest follows in complete analogy to the proof of the approximation property.

For the almost-orthogonality property, suppose $|v\rangle \in H_M^{(n,\delta)}(t')$ and $|w\rangle \in H_M^{(n,\delta)}(t)$ are two arbitrary qubit strings of length n with different approximate halting times $t < t' \in \mathbb{N}$. There is some $l \in \{1, \ldots, L\}$ such that $|w\rangle \in U_\delta(|\psi_l\rangle)$, so $\mathrm{dist}(\mathcal{H}_M^{(n,\delta)}(t), |\psi_l\rangle) < \delta < \tilde\delta$. Since $I(K, N, |\tilde\varphi_1\rangle, \ldots, |\tilde\varphi_K\rangle, |\varphi_1\rangle, \ldots, |\varphi_N\rangle, d, \Delta, \delta, \tilde\Delta, \tilde\delta) = (1, \mathcal{H}_M^{(n,\delta)}(t))$ at step (5) of the computation of $\mathcal{H}_M^{(n,\delta)}(t)$, it follows from the definition of I that there is no $m \in \mathbb{N}$ such that $|\psi_l\rangle = |\tilde\varphi_m\rangle$ for the sets defined in step (3) of the algorithm above. Thus, $B(|\psi_l\rangle, \delta, 18\,\delta, t, s_M) = 1$, and by definition of B it follows that $U_\delta(|\psi_l\rangle)$ must be $(18\,\delta)$-t-halting for M, so there is some vector $|\tilde{w}\rangle \in U_\delta(\psi_l\rangle) \cap S_n$ which is $(18\,\delta)$-t-halting for M and satisfies $\|\,|w\rangle - |\tilde{w}\rangle\| \leq \|\,|\tilde{w}\rangle - |\psi_l\rangle\| + \|\,|\psi_l\rangle - |w\rangle\| < 2\delta$. Analogously, there is some vector $|\tilde{v}\rangle \in S_n$ which is $(18\,\delta)$-t'-halting for M and satisfies $\|\,|v\rangle - |\tilde{v}\rangle\| < 2\delta$.

From the definition of the trace distance for pure states (see [18, (9.99)] and of the ε-t-halting property in Definition 3.3 together with Lemma 1.3 and Lemma 1.5, it follows that

$$\begin{aligned}
\sqrt{1 - |\langle w|v\rangle|^2} &= \|\,|w\rangle\langle w| - |v\rangle\langle v|\,\|_{\mathrm{Tr}} \\
&\geq \|\,|\tilde{w}\rangle\langle\tilde{w}| - |\tilde{v}\rangle\langle\tilde{v}|\,\|_{\mathrm{Tr}} \\
&\quad -\|\,|w\rangle\langle w| - |\tilde{w}\rangle\langle\tilde{w}\|\,\|_{\mathrm{Tr}} \\
&\quad -\|\,|v\rangle\langle v| - |\tilde{v}\rangle\langle\tilde{v}|\,\|_{\mathrm{Tr}} \\
&\geq \big|\langle q_f|M_{\mathbf{C}}^t(|\tilde{w}\rangle\langle\tilde{w}|)|q_f\rangle \\
&\qquad -\langle q_f|M_{\mathbf{C}}^{t}(|\tilde{v}\rangle\langle\tilde{v}|)|q_f\rangle\big| \\
&\quad -\|\,|w\rangle - |\tilde{w}\rangle\| - \|\,|v\rangle - |\tilde{v}\rangle\| \\
&\geq 1 - 36\,\delta - 2\delta - 2\delta = 1 - 40\,\delta. \qquad (9)
\end{aligned}$$

This proves the almost-orthogonality property. □

Corollary 3.9 (Dimension Bound for Halting Spaces): If $\delta < \frac{1}{80}\,2^{-2n}$, then $\sum_{t\in\mathbb{N}} \dim \mathcal{H}_M^{(n,\delta)}(t) \leq 2^n$.

Proof. Suppose that $\sum_{t\in\mathbb{N}} \dim \mathcal{H}_M^{(n,\delta)}(t) > 2^n$. Let $\{|\varphi_i\rangle\}_{i=1}^{2^n+1}$ be a set of orthonormal basis vectors from the spaces $\mathcal{H}_M^{(n,\delta)}(t)$. By construction and by the almost-orthogonality property of Theorem 3.8, it follows that $|\langle\varphi_i|\varphi_j\rangle| \leq 4\sqrt{5\delta} < 2^{-n} = \frac{1}{(2^n+1)-1}$ for every $i \neq j$. Lemma 1.1 yields $\dim U \geq 2^n + 1$ for $U := \mathrm{span}\{|\varphi_i\rangle\}_{i=1}^{2^n+1} \subset \left(\mathbb{C}^2\right)^{\otimes n}$, but $\dim\left(\mathbb{C}^2\right)^{\otimes n} = 2^n$, which is a contradiction. □

C. Compression, Decompression, and Coding

In this subsection, we define some compression and coding algorithms that will be used in the construction of the strongly universal QTM.

Definition 3.10 (Standard (De-)Compression): Let $U \subset \mathcal{H}_n$ be a linear subspace with $\dim U = N$. Let $P_U \in \mathcal{B}(\mathcal{H}_n)$ be the orthogonal projector onto U, and let $\{|e_i\rangle\}_{i=1}^{2^n}$ be the computational basis of $\mathcal{H}_n$. The result of applying the Gram-Schmidt orthonormalization procedure to the vectors $\{|\tilde{u}_i\rangle\}_{i=1}^{2^n} = \{P_U|e_i\rangle\}_{i=1}^{2^n}$ (dropping every null vector) is called the *standard basis* $\{|u_1\rangle, \ldots, |u_N\rangle\}$ of U. Let $|f_i\rangle$ be the i-th computational basis vector of $\mathcal{H}_{\lceil\log_2 N\rceil}$. The *standard compression* $\mathcal{C}_U : U \to \mathcal{H}_{\lceil\log_2 N\rceil}$ is then defined by linear extension of $\mathcal{C}_U(|u_i\rangle) := |f_i\rangle$ for $1 \leq i \leq N$, that is, $\mathcal{C}_U$ isometrically embeds U into $\mathcal{H}_{\lceil\log_2 N\rceil}$. A linear isometric map $\mathcal{D}_U : \mathcal{H}_{\lceil\log_2 N\rceil} \to \mathcal{H}_n$ will be called a *standard decompression* if it holds that

$$\mathcal{D}_U \circ \mathcal{C}_U = \mathbf{1}_U \ .$$

It is clear that there exists a classical algorithm that, given a description of U (e.g. a list of basis vectors $\{|u_i\rangle\}_{i=1}^{\dim U} \subset \left(\mathbb{C}^2\right)^{\otimes n}_{\mathbb{Q}}$), can effectively compute (classically) an approximate description of the standard basis of U. Moreover, a quantum Turing machine can effectively apply a standard decompression map to its input:

Lemma 3.11 (Q-Standard Decompression Algorithm): There is a QTM $\mathfrak{D}$ which, given a description[6] of a subspace $U \subset \mathcal{H}_n$, the integer $n \in \mathbb{N}$, some $\delta \in \mathbb{Q}^+$, and a quantum state $|\psi\rangle \in \mathcal{H}_{\lceil\log_2\dim U\rceil}$, outputs some state $|\varphi\rangle \in \mathcal{H}_n$ with the property that $\|\,|\varphi\rangle - \mathcal{D}_U|\psi\rangle\| < \delta$, where $\mathcal{D}_U$ is some standard decompression map.

Proof. Consider the map $A : \mathcal{H}_{\lceil\log_2\dim U\rceil} \to \mathcal{H}_n$, given by $A|v\rangle := |0\rangle^{\otimes(n-\lceil\log_2\dim U\rceil)} \otimes |v\rangle$. The map A appends zeroes to a vector; it maps the computational basis vectors of $\mathcal{H}_{\lceil\log_2\dim U\rceil}$ to the lexicographically first computational basis vectors of $\mathcal{H}_n$. The QTM $\mathfrak{D}$ starts by applying this map A to the input state $|\psi\rangle$ by appending zeroes on its tape, creating a state $|\tilde{\psi}\rangle := |0\rangle^{\otimes(n-\lceil\log_2\dim U\rceil)} \otimes |\psi\rangle \in \mathcal{H}_n$.

Afterwards, it applies (classically) the Gram-Schmidt orthonormalization procedure to the list of vectors $\{|\tilde{u}_1\rangle, \ldots, |\tilde{u}_{\dim U}\rangle, |e_1\rangle, \ldots, |e_{2^n}\rangle\} \subset \left(\mathbb{C}^2\right)^{\otimes n}_{\mathbb{Q}}$, where the vectors $\{|\tilde{u}_i\rangle\}_{i=1}^{\dim U}$ are the basis vectors of U given in the input, and the vectors $\{|e_i\rangle\}_{i=1}^{2^n}$ are the computational basis vectors of $\mathcal{H}_n$. Since every vector has rational entries (i.e. is an element of $\left(\mathbb{C}^2\right)^{\otimes n}_{\mathbb{Q}}$), the Gram-Schmidt procedure can be applied exactly, resulting in a list $\{|u_i\rangle\}_{i=1}^{2^n}$ of basis vectors of $\mathcal{H}_n$ which have entries that are square roots of rational numbers. Note that by construction, the vectors $\{|u_i\rangle\}_{i=1}^{\dim U}$ are the standard basis vectors of U that have been defined in Definition 3.10.

Let V be the unitary $2^n \times 2^n$-matrix that has the vectors $\{|u_i\rangle\}_{i=1}^{2^n}$ as its column vectors. The algorithm continues by computing a rational approximation $\tilde{V}$ of V such that the entries satisfy $|\tilde{V}_{ij} - V_{ij}| < \frac{\delta}{2^{n+1}(10\sqrt{2^n})^{2^n}}$, and thus, in operator norm, it holds $\|\tilde{V} - V\| < \frac{\delta}{2(10\sqrt{2^n})^{2^n}}$. Bernstein and Vazirani [3, Sec. 6] have shown that there are QTMs that can carry out an ε-approximation of a desired unitary transformation V on their tapes if given a matrix $\tilde{V}$ as input that is within distance $\frac{\varepsilon}{2(10\sqrt{d})^d}$ of the $d \times d$-matrix V. This is exactly the case here[7], with $d = 2^n$ and $\varepsilon = \delta$, so let the $\mathfrak{D}$ apply V within δ on its tape to create the state $|\varphi\rangle \in \mathcal{H}_n$ with $\|\,|\varphi\rangle - V|\tilde{\psi}\rangle\| = \|\,|\varphi\rangle - V \circ A|\psi\rangle\| < \delta$. Note that the map $V \circ A$ is a standard decompression map (as defined in Definition 3.10), since for every $i \in \{1, \ldots, \dim U\}$ it holds that

$$V \circ A \circ \mathcal{C}_U|u_i\rangle = V \circ A|f_i\rangle = V|e_i\rangle = |u_i\rangle \ ,$$

where the vectors $|f_i\rangle$ are the computational basis vectors of $\mathcal{H}_{\lceil\log_2\dim U\rceil}$. □

The next lemma will be useful for coding the "classical part" of a halting qubit string. The "which subspace" information will be coded into a classical string $c_i \in \{0,1\}^*$ whose length $\ell_i \in \mathbb{N}_0$ depends on the dimension of the corresponding halting space $\mathcal{H}_M^{(n,\delta)}(t_i)$. The dimensions of the halting spaces

[6](a list of linearly independent vectors $\{|\tilde{u}_1\rangle, \ldots, |\tilde{u}_{\dim U}\rangle\} \subset U \cap \left(\mathbb{C}^2\right)^{\otimes n}_{\mathbb{Q}}$)

[7]Note that we consider $\mathcal{H}_n$ as a subspace of an n-cell tape segment Hilbert space $\left(\mathbb{C}^{\{0,1,\#\}}\right)^{\otimes n}$, and we demand V to leave blanks $|\#\rangle$ invariant.

$\left(\dim \mathcal{H}_M^{(n,\delta)}(t_1), \dim \mathcal{H}_M^{(n,\delta)}(t_2), \ldots\right)$ can be computed one after the other, but the complete list of the code word lengths ℓ_i is incomputable due to the undecidability of the halting problem. Since most well-known prefix codes (like Huffman code, see [19]) start by initially sorting the code word lengths in decreasing order, and thus require complete knowledge of the whole list of code word lengths in advance, they are useless for our purpose. We thus give an easy algorithm that constructs the code words one after the other, such that code word c_i depends only on the previously given lengths $\ell_1, \ell_2, \ldots, \ell_i$. We call this "blind prefix coding", because code words are assigned sequentially without looking at what is coming next.

Lemma 3.12 (Blind Prefix Coding): Let $\{\ell_i\}_{i=1}^N \subset \mathbb{N}_0$ be a sequence of natural numbers (code word lengths) that satisfies the Kraft inequality $\sum_{i=1}^N 2^{-\ell_i} \leq 1$. Then the following ("blind prefix coding") algorithm produces a list of code words $\{c_i\}_{i=1}^N \subset \{0,1\}^*$ with $\ell(c_i) = \ell_i$, such that the i-th code word only depends on ℓ_i and the previously chosen codewords $c_1, \ldots, c_{i-1}$:

- Start with $c_1 := 0^{\ell_1}$, i.e. c_1 is the string consisting of ℓ_1 zeroes;
- for $i = 2, \ldots, N$ recursively, let c_i be the first string in lexicographical order of length $\ell(c_i) = \ell_i$ that is no prefix or extension of any of the previously assigned code words $c_1, \ldots, c_{i-1}$.

Proof. We omit the lengthy, but simple proof; it is based on identifying the binary code words with subintervals of $[0,1)$ as explained in [13]. We also remark that the content of this lemma is given in [19, Thm. 5.2.1] without proof as an example for a prefix code. □

D. Proof of the Main Theorems

To simplify the proof of Main Theorem 1.1, we show now that it is sufficient to consider fixed-length QTMs only:

Lemma 3.13 (Fixed-Length QTMs are Sufficient): For every QTM M, there is a fixed-length QTM $\tilde{M}$ such that for every $\rho \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ there is a fixed-length qubit string $\tilde{\rho} \in \bigcup_{n \in \mathbb{N}_0} \mathcal{T}_1^+(\mathcal{H}_n)$ such that $M(\rho) = \tilde{M}(\tilde{\rho})$ and $\ell(\tilde{\rho}) \leq \ell(\rho) + 1$.

Proof. Since $\dim \mathcal{H}_{\leq n} = 2^{n+1} - 1$, there is an isometric embedding of $\mathcal{H}_{\leq n}$ into $\mathcal{H}_{n+1}$. One example is the map V_n, which is defined as $V_n|e_i\rangle := |f_i\rangle$ for $i \in \{1, \ldots, 2^{n+1} - 1\}$, where $|e_i\rangle$ and $|f_i\rangle$ denote the computational basis vectors (in lexicographical order) of $\mathcal{H}_{\leq n}$ and $\mathcal{H}_{n+1}$ respectively. As $\mathcal{H}_{n+1} \subset \mathcal{H}_{\leq(n+1)}$ and $\mathcal{H}_{\leq n} \subset \mathcal{H}_{\leq(n+1)}$, we can extend V_n to a unitary transformation U_n on $\mathcal{H}_{\leq(n+1)}$, mapping computational basis vectors to computational basis vectors.

The fixed-length QTM $\tilde{M}$ works as follows, given some fixed-length qubit string $\tilde{\rho} \in \mathcal{T}_1^+(\mathcal{H}_{n+1})$ on its input tape: First, it determines $n + 1 = \ell(\tilde{\rho})$ by detecting the first blank symbol $\#$. Afterwards, it computes a description of the unitary transformation U_n^* and applies it to the qubit string $\tilde{\rho}$ by permuting the computational basis vectors in the $(n+1)$-block of cells corresponding to the Hilbert space $\left(\mathbb{C}^{\{0,1,\#\}}\right)^{\otimes(n+1)}$. Finally, it calls the QTM M to continue the computation on input $\rho := U_n^* \tilde{\rho} U_n$. If M halts, then the output will be $M(\rho)$. □

Proof of Theorem 1.1. First, we show how the input σ_M for the strongly universal QTM $\mathfrak{U}$ is constructed from the input σ for M. Fix some QTM M and input length $n \in \mathbb{N}_0$, and let $\varepsilon_0 := \frac{1}{81} 2^{-2n}$. Define the halting time sequence $\{t_M^{(n)}(i)\}_{i=1}^N$ as the set of all integers $t \in \mathbb{N}$ such that $\dim \mathcal{H}_M^{(n,\varepsilon_0)}(t) \geq 1$, ordered such that $t_M^{(n)}(i) < t_M^{(n)}(i+1)$ for every i. The number N is in general incomputable, but must be somewhere between 0 and 2^n due to Corollary 3.9.

For every $i \in \{1, \ldots, N\}$, define the code word length $\ell_i^{(M,n)}$ as

$$\ell_i^{(M,n)} := n + 1 - \left\lceil \log_2 \dim \mathcal{H}_M^{(n,\varepsilon_0)} \left(t_M^{(n)}(i) \right) \right\rceil \ .$$

This sequence of code word lengths satisfies the Kraft inequality:

$$\begin{aligned}
\sum_{i=1}^N 2^{-\ell_i^{(M,n)}} &= 2^{-n} \sum_{i=1}^N 2^{\left\lceil \log_2 \dim \mathcal{H}_M^{(n,\varepsilon_0)} \left(t_M^{(n)}(i) \right) \right\rceil - 1} \\
&\leq 2^{-n} \sum_{i=1}^N \dim \mathcal{H}_M^{(n,\varepsilon_0)} \left(t_M^{(n)}(i) \right) \\
&= 2^{-n} \sum_{t \in \mathbb{N}} \dim \mathcal{H}_M^{(n,\varepsilon_0)}(t) \leq 1 \ ,
\end{aligned}$$

where in the last inequality, Corollary 3.9 has been used. Let $\left\{c_i^{(M,n)}\right\}_{i=1}^N \subset \{0,1\}^*$ be the blind prefix code corresponding to the sequence $\left\{\ell_i^{(M,n)}\right\}_{i=1}^N$ which has been constructed in Lemma 3.12.

In the following, we use the space $\mathcal{H}_M^{(n,\varepsilon_0)}(t)$ as some kind of "reference space" i.e. we construct our QTM $\mathfrak{U}$ such that it expects the standard compression of states $|\psi\rangle \in \mathcal{H}_M^{(n,\varepsilon_0)}(t)$ as part of the input. If the desired accuracy parameter δ is smaller than ε_0, then some "fine-tuning" must take place, unitarily mapping the state $|\psi\rangle \in \mathcal{H}_M^{(n,\varepsilon_0)}(t)$ into halting spaces of smaller accuracy parameter. In the next paragraph, these unitary transformations are constructed.

Recursively, for $k \in \mathbb{N}$, define $\varepsilon_k := \frac{1}{80} \varepsilon_M^{(n,\varepsilon_{k-1})}(t)$. Since $\varepsilon_M^{(n,\delta)}(t) \leq 18\delta$ by construction of the algorithm in Definition 3.6, we have $\varepsilon_k \leq \left(\frac{18}{80}\right)^k \cdot \varepsilon_0 \xrightarrow{k \to \infty} 0$. It follows from the approximation property of Theorem 3.8 together with Lemma 1.4 that $\dim \mathcal{H}_M^{(n,\varepsilon_k)}(t) \geq \dim \mathcal{H}_M^{(n)}(t)$. The similarity property and Lemma 1.4 tell us that $\dim \mathcal{H}_M^{(n,\varepsilon_{k-1})}(t) \geq \dim \mathcal{H}_M^{(n,\varepsilon_k)}(t)$ for every $k \in \mathbb{N}$, and there exist isometries $U_k : \mathcal{H}_M^{(n,\varepsilon_k)}(t) \to \mathcal{H}_M^{(n,\varepsilon_{k-1})}(t)$ that, for k large enough, satisfy

$$\|U_k - \mathbf{1}\| < \frac{8}{3} \sqrt{\frac{11}{2} \varepsilon_{k-1}} \left(\frac{5}{2}\right)^{2^n} \leq \mathrm{const}_n \cdot \left(\frac{18}{80}\right)^{\frac{k}{2}} . \quad (10)$$

Let now $d := \lim_{k \to \infty} \dim \mathcal{H}_M^{(n,\varepsilon_k)}(t)$ and $c := \min\left\{k \in \mathbb{N} \mid \dim \mathcal{H}_M^{(n,\varepsilon_k)}(t) = d\right\}$. For any choice of the transformations U_k (they are not unique), let

$$\tilde{\mathcal{H}}_M^{(n,\varepsilon_k)}(t) := \begin{cases} U_{k+1}U_{k+2}\ldots U_c\mathcal{H}_M^{(n,\varepsilon_c)}(t) & \text{if } k < c \ , \\ \mathcal{H}_M^{(n,\varepsilon_k)}(t) & \text{if } k \geq c \ . \end{cases}$$

It follows that the spaces $\tilde{\mathcal{H}}_M^{(n,\varepsilon_k)}(t)$ all have the same dimension for every $k \in \mathbb{N}_0$, and that $\tilde{\mathcal{H}}_M^{(n,\varepsilon_k)}(t) \subset \mathcal{H}_M^{(n,\varepsilon_k)}(t)$. Define the unitary operators $\tilde{U}_k := U_k \restriction \tilde{\mathcal{H}}_M^{(n,\varepsilon_k)}(t)$, then $\|\tilde{U}_k^* - \mathbf{1}\| \leq \|U_k - \mathbf{1}\|$, and so the sum $\sum_{k=1}^\infty \|\tilde{U}_k^* - \mathbf{1}\|$ converges. Due to Lemma 1.2, the product $U := \prod_{k=1}^\infty \tilde{U}_k^*$ converges to an isometry $U : \tilde{\mathcal{H}}_M^{(n,\varepsilon_0)}(t) \to \mathcal{H}_n$. It follows from the approximation property in Theorem 3.8 that $\mathcal{H}_M^{(n)}(t) \subset \mathrm{ran}(U)$, so we can define a unitary map $U^{-1} : \mathrm{ran}(U) \to \tilde{\mathcal{H}}_M^{(n,\varepsilon_0)}(t)$ by $U^{-1}(Ux) := x$, and $\mathcal{H}_M^{(n)}(t) \subset \mathrm{dom}(U^{-1})$.

Due to Lemma 3.13, it is sufficient to consider fixed-length QTMs M only, so we can assume that our input σ is a fixed-length qubit string. Suppose $M(\sigma)$ is defined, and let $\tau \in \mathbb{N}$ be the corresponding halting time for M. Assume for the moment that $\sigma = |\psi\rangle\langle\psi|$ is a pure state, so $|\psi\rangle \in H_M^{(n)}(\tau)$. Recall the definition of the halting time sequence; it follows that there is some $i \in \mathbb{N}$ such that $\tau = t_M^{(n)}(i)$. Let

$$|\psi^{(M,n)}\rangle := |c_i^{(M,n)}\rangle \otimes \mathcal{C}_{\mathcal{H}_M^{(n,\varepsilon_0)}(\tau)} U^{-1}|\psi\rangle \ ,$$

that is, the blind prefix code of the halting number i, followed by the standard compression (as constructed in Definition 3.10) of some approximation $U^{-1}|\psi\rangle$ of $|\psi\rangle$ that is in the subspace $\mathcal{H}_M^{(n,\varepsilon_0)}(\tau)$. Note that

$$\begin{aligned} \ell\left(|\psi^{(M,n)}\rangle\right) &= \ell\left(c_i^{(M,n)}\right) + \ell\left(\mathcal{C}_{\mathcal{H}_M^{(n,\varepsilon_0)}(\tau)} U^{-1}|\psi\rangle\right) \\ &= \ell_i^{(M,n)} + \left\lceil \log_2 \dim \mathcal{H}_M^{(n,\varepsilon_0)}(\tau) \right\rceil = n+1 \ . \end{aligned}$$

If $\sigma = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ is a mixed fixed-length qubit string which is τ-halting for M, every convex component $|\psi_k\rangle$ must also be τ-halting for M, and it makes sense to define $\sigma^{(M,n)} := \sum_k \lambda_k |\psi_k^{(M,n)}\rangle\langle\psi_k^{(M,n)}|$, where every $|\psi_k^{(M,n)}\rangle$ (and thus $\sigma^{(M,n)}$) starts with the same classical code word $c_i^{(M,n)}$, and still $\sigma^{(M,n)} \in \mathcal{T}_1^+(\mathcal{H}_{n+1})$.

The strongly universal QTM $\mathfrak{U}$ expects input of the form

$$\left(s_M \otimes \sigma^{(M,n)}, \delta\right) =: (\sigma_M, \delta) \ , \qquad (11)$$

where $s_M \in \{0,1\}^*$ is a self-delimiting description of the QTM M. We will now give a description of how $\mathfrak{U}$ works; meanwhile, we will always assume that the input is of the expected form (11) and also that the input σ is a *pure* qubit string $|\psi\rangle\langle\psi|$ (we discuss the case of mixed input qubit strings σ afterwards):

- Read the parameter δ and the description s_M.
- Look for the first blank symbol # on the tape to determine the length $\ell(\sigma^{(M,n)}) = n+1$.
- Compute the halting time τ. This is achieved as follows:
  (1) Set $t := 1$ and $i := 0$.
  (2) Compute a description of $\mathcal{H}_M^{(n,\varepsilon_0)}(t)$. If $\dim \mathcal{H}_M^{(n,\varepsilon_0)}(t) = 0$, then go to step (5).
  (3) Set $i := i+1$ and set $\ell_i^{(M,n)} := n+1-\left\lceil \log_2 \dim \mathcal{H}_M^{(n,\varepsilon_0)}(t) \right\rceil$. From the previously computed code word lengths $\ell_j^{(M,n)}$ $(1 \leq j \leq i)$, compute the corresponding blind prefix code word $c_i^{(M,n)}$. Bit by bit, compare the code word $c_i^{(M,n)}$ with the prefix of $\sigma^{(M,n)}$. As soon as any difference is detected, go to step (5).
  (4) The halting time is $\tau := t$. Exit.
  (5) Set $t := t+1$ and go back to step (2).
- Let $|\tilde{\psi}\rangle$ be the rest of the input, i.e. $\sigma^{(M,n)} =: |c_i^{(M,n)}\rangle\langle c_i^{(M,n)}| \otimes |\tilde{\psi}\rangle\langle\tilde{\psi}|$ (up to a phase, this means that $|\tilde{\psi}\rangle = \mathcal{C}_{\mathcal{H}_M^{(n,\varepsilon_0)}(\tau)} U^{-1}|\psi\rangle$). Apply the quantum standard decompression algorithm $\mathfrak{D}$ given in Lemma 3.11, i.e. compute $|\tilde{\varphi}\rangle := \mathfrak{D}\left(\mathcal{H}_M^{(n,\varepsilon_0)}(\tau), n, \frac{\delta}{3}, |\tilde{\psi}\rangle\right)$. Then,
$$\left\| \, |\tilde{\varphi}\rangle - \mathcal{D}_{\mathcal{H}_M^{(n,\varepsilon_0)}(\tau)} |\tilde{\psi}\rangle \right\| = \left\| \, |\tilde{\varphi}\rangle - U^{-1}|\psi\rangle \right\| < \frac{\delta}{3} \ .$$
- Compute an approximation $V : \mathcal{H}_n \to \mathcal{H}_n$ of a unitary extension of U with $\left\| U - V \restriction \tilde{\mathcal{H}}_M^{(n,\varepsilon_0)}(\tau) \right\| < \frac{\delta/3}{2(10\sqrt{2^n})^{2^n}} =: \varepsilon$, where U is some "fine-tuning map" as constructed above. This can be achieved as follows:
  – Choose $N \in \mathbb{N}$ large enough such that $\sum_{k=N+1}^\infty \mathrm{const}_n \cdot \left(\frac{18}{80}\right)^{\frac{k}{2}} < \frac{\varepsilon}{2}$, where $\mathrm{const}_n \in \mathbb{R}$ is the constant defined in Equation (10).
  – For every $k \in \{1, \ldots, N\}$, find matrices $V_k : \mathcal{H}_n \to \mathcal{H}_n$ that approximate the forementioned[8] isometries $U_k : \mathcal{H}_M^{(n,\varepsilon_k)}(t) \to \mathcal{H}_M^{(n,\varepsilon_{k-1})}(t)$ such that
$$\left\| \prod_{k=1}^N \tilde{U}_k^* - \prod_{k=1}^N V_k^* \restriction \tilde{\mathcal{H}}_M^{(n,\varepsilon_0)}(t) \right\| < \frac{\varepsilon}{2} \ .$$

  Setting $V := \prod_{k=1}^N V_k^*$ will work as desired, since
$$\begin{aligned} \left\| \prod_{k=1}^N \tilde{U}_k^* - U \right\| &\leq \sum_{k=N+1}^\infty \|U_k - \mathbf{1}\| \\ &\leq \sum_{k=N+1}^\infty \mathrm{const}_n \cdot \left(\frac{18}{80}\right)^{\frac{k}{2}} < \frac{\varepsilon}{2} \end{aligned}$$
  due to Equation (10) and the proof of Lemma 1.2.
- Use V to carry out a $\frac{\delta}{3}$-approximation of a unitary extension $\tilde{U}$ of U on the state $|\tilde{\varphi}\rangle$ on the tape (the reason why this is possible is explained in the proof of Lemma 3.11). This results in a vector $|\varphi\rangle$ with the property that $\| \, |\varphi\rangle - \tilde{U}|\tilde{\varphi}\rangle \| < \frac{\delta}{3}$.
- Simulate M on input $|\varphi\rangle\langle\varphi|$ for τ time steps within an accuracy of $\frac{\delta}{3}$, that is, compute an output track state $\rho_{\mathbf{O}} \in \mathcal{T}_1^+(\mathcal{H}_{\mathbf{O}})$ with $\|\rho_{\mathbf{O}} - M_{\mathbf{O}}^\tau(|\varphi\rangle\langle\varphi|)\|_{\mathrm{Tr}} < \frac{\delta}{3}$, move this state to the own output track and halt. (It has been shown by Bernstein and Vazirani in [3] that there are QTMs that can do a simulation in this way.)

[8]The isometries U_k are not unique, so they can be chosen arbitrarily, except for the requirement that Equation (10) is satisfied, and that every U_k depends only on $\mathcal{H}_M^{(n,\varepsilon_k)}(t)$ and $\mathcal{H}_M^{(n,\varepsilon_{k-1})}(t)$ and not on other parameters.

Let $\sigma_M := s_M \otimes \sigma^{(M,n)}$. Using the contractivity of the trace distance with respect to quantum operations and Lemma 1.3, we get

$$\begin{aligned}
\|\mathfrak{U}(\sigma_M,\delta) &- M(|\psi\rangle\langle\psi|)\|_{\mathrm{Tr}} = \\
&= \|\mathcal{R}(\rho_{\mathbf{O}}) - \mathcal{R}(M^\tau_{\mathbf{O}}(|\psi\rangle\langle\psi|))\|_{\mathrm{Tr}} \\
&\leq \|\rho_{\mathbf{O}} - M^\tau_{\mathbf{O}}(|\varphi\rangle\langle\varphi|)\|_{\mathrm{Tr}} \\
&\quad + \|M^\tau_{\mathbf{O}}(|\varphi\rangle\langle\varphi|) - M^\tau_{\mathbf{O}}(|\psi\rangle\langle\psi|)\|_{\mathrm{Tr}} \\
&< \frac{\delta}{3} + \||\varphi\rangle\langle\varphi| - |\psi\rangle\langle\psi|\|_{\mathrm{Tr}} \\
&\leq \frac{\delta}{3} + \|\,|\varphi\rangle - |\psi\rangle\| \\
&\leq \frac{\delta}{3} + \|\,|\varphi\rangle - \tilde{U}|\tilde{\varphi}\rangle\| + \|\tilde{U}|\tilde{\varphi}\rangle - |\psi\rangle\| \\
&< \frac{2}{3}\delta + \left\|\,|\tilde{\varphi}\rangle - \tilde{U}^*|\psi\rangle\right\| < \delta\ .
\end{aligned}$$

This proves the claim for pure inputs $\sigma = |\psi\rangle\langle\psi|$. If $\sigma = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$ is a mixed qubit string as explained right before Equation (11), the result just proved holds for every convex component of σ by the linearity of M, i.e. $\|\rho_k - M(|\psi_k\rangle\langle\psi_k|)\|_{\mathrm{Tr}} < \delta$, and the assertion of the theorem follows from the joint convexity of the trace distance and the observation that $\mathfrak{U}$ takes the same number of time steps for every convex component $|\psi_k\rangle\langle\psi_k|$. □

This proof relies on the existence of a universal QTM $\mathcal{U}$ in the sense of Bernstein and Vazirani as given in Equation (1). Nevertheless, the proof does not imply that every QTM that satisfies (1) is automatically strongly universal in the sense of Theorem 1.1; for example, we can construct a QTM $\mathcal{U}$ that always halts after T simulated steps of computation on input $(s_M, T, \delta, |\psi\rangle)$ and that does not halt at all if the input is not of this form. So formally,

$$\{\mathcal{U}\text{ QTM universal by (1)}\} \supsetneq \{\mathfrak{U}\text{ QTM strongly universal}\}.$$

Proposition 3.14 (Parameter Strongly Universal QTM): There is a fixed-length quantum Turing machine $\mathfrak{U}$ with the property of Theorem 1.1 that additionally satisfies the following: For every QTM M and every qubit string $\sigma \in \mathcal{T}_1^+\left(\mathcal{H}_{\{0,1\}^*}\right)$, there is a qubit string $\sigma_M \in \mathcal{T}_1^+\left(\mathcal{H}_{\{0,1\}^*}\right)$ such that

$$\|\mathfrak{U}(\sigma_M,k) - M(\sigma,2k)\|_{\mathrm{Tr}} < \frac{1}{2k} \qquad \text{for every } k \in \mathbb{N}$$

if $M(\sigma,2k)$ is defined for every $k \in \mathbb{N}$, where the length of σ_M is bounded by $\ell(\sigma_M) \leq \ell(\sigma) + c_M$, and $c_M \in \mathbb{N}$ is a constant depending only on M.

One might first suspect that this proposition is an easy corollary of Theorem 1.1, but this is not true. The problem is that the computation of $M(\sigma,k)$ may take a different number of time steps τ for different k (typically, $\tau \to \infty$ for $k \to \infty$). Just using the result of Theorem 1.1 would give a corresponding qubit string σ_M that depends on k, but here we demand that the qubit string σ_M is the *same* for every k, which is important for the proof of Theorem 1.2 to fit the definition of $QC^{\searrow 0}$.

Thus, we have to give a new proof that is different from the proof of Theorem 1.1. Nevertheless, the new proof relies essentially on the same ideas and techniques; for this reason, we will only sketch the proof and omit most of the details.

Draft of Proof. In analogy to Definition 3.1, we can define halting spaces $\mathcal{H}_M^{(n)}(t_1,t_2,\ldots,t_j)$ as the linear span of

$$H_M^{(n)}(t_1,t_2,\ldots,t_j) := \{|\psi\rangle \in \mathcal{H}_n \mid (|\psi\rangle\langle\psi|, i) \text{ is } t_i\text{-halting for } M\ (1 \leq i \leq j)\}.$$

Again, we have $\mathcal{H}_M^{(n)}\left((t_i)_{i=1}^j\right) \perp \mathcal{H}_M^{(n)}\left((t_i')_{i=1}^j\right)$ if $t \neq t'$, and now it also holds that $\mathcal{H}_M^{(n)}(t_1,\ldots,t_j,t_{j+1}) \subset \mathcal{H}_M^{(n)}(t_1,\ldots,t_j)$ for every $j \in \mathbb{N}$. Moreover, we can define certain δ-approximations $\mathcal{H}_M^{(n,\delta)}(t_1,\ldots,t_j)$. We will not get into detail and just claim that such a definition can be found in a way such that these δ-approximations share enough properties with their counterparts from Definition 3.6 to make the algorithm given below work.

While the QTM $\mathfrak{U}$ can apply every unitary transformation on its tapes within arbitrary accuracy, there are some unitaries U that $\mathfrak{U}$ can even apply *exactly* (call such transformations "$\mathfrak{U}$-exact unitaries"). For example, to allow our machine to perfectly simulate classical reversible Turing machines, we have to construct it in a way such that it can permute the 0 and 1-symbols on its tapes (in the computational basis) without any error. If $\mathfrak{U}$ is constructed such that it can additionally apply a finite, discrete, universal set of unitary operations exactly (see, for example, [18, 4.5.3] for such sets), there will be a dense set of $\mathfrak{U}$-exact unitaries.

Call a projector $P \in \mathcal{B}\left(\left(\mathbb{C}^2\right)^{\otimes n}\right)$ $\mathfrak{U}$-exact, if there exists a $\mathfrak{U}$-exact unitary U such that P can be written as $P = \sum_i |\psi_i\rangle\langle\psi_i|$ and U maps every vector $|\psi_i\rangle$ to a computational basis vector of $\left(\mathbb{C}^2\right)^{\otimes n}$. Note that if P is a $\mathfrak{U}$-exact projector, then $\mathfrak{U}$ can do exact projective measurements described by P.

We are now going to describe how a machine $\mathfrak{U}$ with the properties given in the assertion of the proposition works. It expects input of the form $\left(f \otimes s_M \otimes \sigma^{(M,n)}, k\right)$, where $f \in \{0,1\}$ is a single bit, $s_M \in \{0,1\}^*$ is a self-delimiting description of the QTM M, $\sigma^{(M,n)} \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ is a qubit string, and $k \in \mathbb{N}$ an arbitrary integer. For the same reasons as in the proof of Theorem 1.1, we may without loss of generality assume that the input is a pure qubit string, so $\sigma^{(M,n)} = |\psi^{(M,n)}\rangle\langle\psi^{(M,n)}|$. Moreover, due to Lemma 3.13, we may also assume that M is a fixed-length QTM, and so $\sigma^{(M,n)} \in \mathcal{T}_1^+(\mathcal{H}_n)$ is a fixed-length qubit string.

(1) Read the first bit f of the input. If it is a 0, then proceed with the rest of the input the same way as the QTM that is given in Theorem 1.1. If it is a 1, then proceed with the next step.
(2) Read s_M, read k, and look for the first blank symbol $\#$ to determine the length $n := \ell(\sigma^{(M,n)})$.
(3) Set $j := 1$ and $\delta_0 \in \mathbb{Q}^+$ (depending on n) small enough.
(4) Set $t := 1$.
(5) Compute $\mathcal{H}_M^{(n,\delta_0)}(\tau_1,\ldots,\tau_{j-1},t)$. Find an exact projector $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t)$ with the following properties:
   - $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t') \cdot P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t) = 0$ for every $1 \leq t' < t$,
   - $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t) \leq P_M^{(n)}(\tau_1,\ldots,\tau_{j-1})$,

- the support of $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t)$ is close enough to $\mathcal{H}_M^{(n,\delta_0)}(\tau_1,\ldots,\tau_{j-1},t)$.

(6) Make a measurement described by $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t)$. If $|\psi^{(M,n)}\rangle$ is an element of the support of $P_M^{(n)}(\tau_1,\ldots,\tau_{j-1},t)$, then set $\tau_j := t$ and go to step (7). Otherwise, if $|\psi^{(M,n)}\rangle$ is an element of the orthogonal complement of the support, set $t := t+1$ and go back to step (5).

(7) If $j<2k$, then set $j:=j+1$ and go back to step (4).

(8) Use a unitary transformation V (similar to the transformation V from the proof of Theorem 1.1) to do some "fine-tuning" on $|\psi^{(M,n)}\rangle$, i.e. to transform it closer (depending on the parameter k) to some space $\tilde{\mathcal{H}}_M^{(n)}(\tau_1,\ldots,\tau_j)\supset\mathcal{H}_M^{(n)}(\tau_1,\ldots,\tau_j)$ containing the exactly halting vectors. Call the resulting vector $|\tilde{\psi}^{(M,n)}\rangle := V|\psi^{(M,n)}\rangle$.

(9) Simulate M on input $\left(|\tilde{\psi}^{(M,n)}\rangle\langle\tilde{\psi}^{(M,n)}|,2k\right)$ for τ_{2k} time steps within some accuracy that is good enough, depending on k.

Let $\tilde{\mathcal{H}}_M^{(n,\delta_0)}(t_1,\ldots,t_j)$ be the support of $P_M^{(n)}(t_1,\ldots,t_j)$. These spaces (which are computed by the algorithm) have the properties

$$\tilde{\mathcal{H}}_M^{(n,\delta_0)}\left((t_i)_{i=1}^j\right)\quad\perp\quad\tilde{\mathcal{H}}_M^{(n,\delta_0)}\left((t'_i)_{i=1}^j\right)\ \text{ if } t\neq t',$$
$$\tilde{\mathcal{H}}_M^{(n,\delta_0)}(t_1,\ldots,t_j,t_{j+1})\quad\subset\quad\tilde{\mathcal{H}}_M^{(n,\delta_0)}(t_1,\ldots,t_j)\ \forall j\in\mathbb{N},$$

which are the same as those of the exact halting spaces $\mathcal{H}_M^{(n)}(t_1,\ldots,t_j)$. If all the approximations are good enough, then for every $|\psi\rangle\in H_M^{(n)}(t_1,\ldots,t_j)$ there will be a vector $|\psi^{(M,n)}\rangle\in\tilde{\mathcal{H}}_M^{(n,\delta_0)}(t_1,\ldots,t_j)$ such that $\|\,|\psi\rangle - V|\psi^{(M,n)}\rangle\|$ is small. If $|\psi^{(M,n)}\rangle$ is given to $\mathfrak{U}$ as input as shown above, then this algorithm will unambigously find out by measurement with respect to the exact projectors that it computes in step (5) what the halting time of $|\psi\rangle$ is, and the simulation of M will halt after the correct number of time steps with perfect fidelity and an output which is close to the true output $M(\sigma,2k)$. $\square$

Proof of Theorem 1.2. First, we use Theorem 1.1 to prove the second part of Theorem 1.2. Let M be an arbitrary QTM, let $\mathfrak{U}$ be the ("strongly universal") QTM and c_M the corresponding constant from Theorem 1.1. Let $\ell := QC_M^\delta(\rho)$, i.e. there exists a qubit string $\sigma\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with $\ell(\sigma)=\ell$ such that

$$\|M(\sigma)-\rho\|_{\mathrm{Tr}}\leq\delta\ .$$

According to Theorem 1.1, there exists a qubit string $\sigma_M\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with $\ell(\sigma_M)\leq\ell(\sigma)+c_M=\ell+c_M$ such that

$$\|\mathfrak{U}(\sigma_M,\Delta-\delta)-M(\sigma)\|_{\mathrm{Tr}}<\Delta-\delta\ .$$

Thus, $\|\mathfrak{U}(\sigma_M,\Delta-\delta)-\rho\|_{\mathrm{Tr}}<\Delta$, and $\ell(\sigma_M,\Delta-\delta)=\ell(\sigma_M)+\ell(\Delta-\delta)\leq\ell+c_M+c_{\delta,\Delta}$, where $c_{\delta,\Delta}\in\mathbb{N}$ is some constant that only depends on δ and Δ. So $QC_{\mathfrak{U}}^\Delta(\rho)\leq\ell+c_{M,\delta,\Delta}$.

The first part of Theorem 1.2 uses Proposition 3.14. Again, let M be an arbitrary QTM, let $\mathfrak{U}$ be the strongly universal QTM and c_M the corresponding constant from Proposition 3.14. Let $\ell := QC_M^{\searrow 0}(\rho)$, i.e. there exists a qubit string $\sigma\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with $\ell(\sigma)=\ell$ such that

$$\|M(\sigma,k)-\rho\|_{\mathrm{Tr}}\leq\frac{1}{k}\qquad\text{for every } k\in\mathbb{N}\ .$$

According to Proposition 3.14, there exists a qubit string $\sigma_M\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with $\ell(\sigma_M)\leq\ell(\sigma)+c_M=\ell+c_M$ such that

$$\|\mathfrak{U}\left(\sigma_M,k\right)-M\left(\sigma,2k\right)\|_{\mathrm{Tr}}<\frac{1}{2k}\qquad\text{for every } k\in\mathbb{N}\ .$$

Thus, $\|\mathfrak{U}(\sigma_M,k)-\rho\|_{\mathrm{Tr}}\leq\|\mathfrak{U}(\sigma_M,k)-M(\sigma,2k)\|_{\mathrm{Tr}}+\|M(\sigma,2k)-\rho\|_{\mathrm{Tr}}<\frac{1}{2k}+\frac{1}{2k}=\frac{1}{k}$ for every $k\in\mathbb{N}$. So $QC_{\mathfrak{U}}^{\searrow 0}(\rho)\leq\ell+c_M$. $\square$

The construction of $\mathfrak{U}$ is based to a large extent on classical algorithms that identify almost halting input qubit strings. Since it is in general impossible to decide unambigously by classical simulation whether some input qubit string $|\psi\rangle$ is perfectly or only approximately halting for a QTM M, the UQTM $\mathfrak{U}$ will also give some outputs of M which correspond to inputs that are only approximately halting. One could imagine to generalize this construction and to find a program for $\mathfrak{U}$ that searches such almost halting inputs and generates the corresponding outputs on purpose. This leads to the following conjecture:

Conjecture 3.15 (Almost Halting Inputs): Let $\sigma\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ be ε-t-halting for some QTM M with small $\varepsilon>0$ and output $\rho:=\mathcal{R}(M_{\mathbf{O}}^t(\sigma))$. Then there is some qubit string $\tilde{\sigma}\in\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with $\ell(\tilde{\sigma})$ not much larger than $\ell(\sigma)$ such that $\mathfrak{U}(\tilde{\sigma})\approx\rho$.

IV. Summary and Perspectives

While Bernstein and Vazirani [3] have defined QTMs with the purpose to study quantum computational complexity, it has been shown in this paper that QTMs are good for studying quantum Kolmogorov complexity as well. As proved in Theorem 1.1, there is a "strongly universal" QTM $\mathfrak{U}$ that simulates every other QTM until the other QTM has halted, thereby even obeying the strict halting conditions that the control is exactly in the halting state at the halting time, and exactly orthogonal to the halting state before.

In analogy to the classical situation, this makes it possible to prove that quantum Kolmogorov complexity depends on the choice of the strongly universal QTM only up to an additive constant, as shown in Theorem 1.2. In the classical case, this "invariance property" turned out to be the cornerstone for the subsequent development of every aspect of algorithmic information theory. We hope that the results in this paper will be similarly useful for the development of a quantum theory of algorithmic information.

There are some more aspects that can be learned from the proofs of Theorems 1.1 and 1.2. One example is Lemma 3.13 which essentially states that variable-length QTMs are no more interesting then fixed-length QTMs, if the length $\ell(\sigma)$ of an input qubit string σ is defined as in Equation (3). This supports the point of view of Rogers and Vedral [17] to consider the average length $\bar{\ell}(\sigma)$ instead, that is, the expectation value of the length ℓ. Nevertheless, it seems that the main results of this paper generalize to their definition, too.

The construction of the strongly universal QTM $\mathfrak{U}$ in Subsection III-D is such that $\mathfrak{U}$ starts with a completely classical computation, followed by the application of classically selected unitary operations. But the same steps (on the same input) can be done by a machine that has a purely classical control, selecting at each step of the computation a unitary transformation that is applied to an unknown quantum state (that was part of the input) without any measurement. Thus, it seems that at least from the point of view of quantum Kolmogorov complexity QC^δ, it is sufficient to consider machines with a completely classical control. Such machines do not have the problem of "approximate halting" described in Subsection I-A.

There may be many applications for carrying over complexity theory to the quantum case. One exciting perspective is that in a quantum theory of algorithmic complexity, both the inherent notions of "randomness" of quantum theory and "algorithmic randomness" originating from undecidability results will occur (and maybe be related) in a single theory. Moreover, there are many applications of classical complexity that may be generalized to quantum theory, the foremost concerning statistical mechanics (cf. [13]) having immediate analogues in quantum statistical mechanics. Another idea is that quantum Kolmogorov complexity (or rather conditional complexity) might be related to entanglement; say, if ρ^{AB} is a pure state on a bipartite system $\mathcal{H}_A\otimes\mathcal{H}_B$, and $\rho^A:=\mathrm{Tr}_B\rho^{AB}$ and $\rho^B:=\mathrm{Tr}_A\rho^{AB}$ are the local states, then what about the quantity $QC(\rho^{AB}|\rho^A\otimes\rho^B)$ which is in the classical case always bounded by a constant?

APPENDIX

Lemma 1.1 (Inner Product and Dimension Bound): Let $\mathcal{H}$ be a Hilbert space, and let $|\psi_1\rangle,\ldots,|\psi_N\rangle\in\mathcal{H}$ with $\|\,|\psi_i\rangle\|=1$ for every $i\in\{1,\ldots,N\}$, where $2\leq N\in\mathbb{N}$. Suppose that

$$\left|\langle\psi_i|\psi_j\rangle\right|<\frac{1}{N-1}\qquad\text{for every } i\neq j\ .$$

Then, $\dim\mathcal{H}\geq N$.

Proof. We prove the statement by induction in $N\in\mathbb{N}$. For $N=2$, the statement of the theorem is trivial. Suppose the claim holds for some $N\geq 2$, then consider $N+1$ vectors $|\psi_1\rangle,\ldots,|\psi_{N+1}\rangle\in\mathcal{H}$, where $\mathcal{H}$ is an arbitrary Hilbert space. Suppose that $|\langle\psi_i|\psi_j\rangle|<\frac{1}{N}$ for every $i\neq j$. Let $P:=\mathbf{1}-|\psi_{N+1}\rangle\langle\psi_{N+1}|$, then $P|\psi_i\rangle\neq 0$ for every $i\in\{1,\ldots,N\}$, and let

$$|\varphi_i'\rangle:=P|\psi_i\rangle\ ,\qquad |\varphi_i\rangle:=\frac{|\varphi_i'\rangle}{\|\,|\varphi_i'\rangle\|}\ .$$

The $|\varphi_i\rangle$ are normalized vectors in the Hilbert subspace $\tilde{\mathcal{H}}:=\mathrm{ran}(P)$ of $\mathcal{H}$. Since $\|\,|\varphi_i'\rangle\|^2=\langle\psi_i|\psi_i\rangle-|\langle\psi_i|\psi_{N+1}\rangle|^2>1-\frac{1}{N^2}$, it follows that the vectors $|\varphi_i\rangle$ have small inner product: Let $i\neq j$, then

$$\begin{aligned}|\langle\varphi_i|\varphi_j\rangle| &= \frac{1}{\|\,|\varphi_i'\rangle\|\cdot\|\,|\varphi_j'\rangle\|}|\langle\varphi_i'|\varphi_j'\rangle|\\ &< \frac{|\langle\psi_i|\psi_j\rangle-\langle\psi_{N+1}|\psi_j\rangle\langle\psi_i|\psi_{N+1}\rangle|}{\sqrt{1-\frac{1}{N^2}}\sqrt{1-\frac{1}{N^2}}}\\ &< \frac{1}{1-\frac{1}{N^2}}\left(\frac{1}{N}+\frac{1}{N^2}\right)=\frac{1}{N-1}\ .\end{aligned}$$

Thus, $\dim\tilde{\mathcal{H}}\geq N$, and so $\dim\mathcal{H}\geq N+1$. □

Lemma 1.2 (Composition of Unitary Operations): Let $\mathcal{H}$ be a finite-dimensional Hilbert space, let $(V_i)_{i\in\mathbb{N}}$ be a sequence of linear subspaces of $\mathcal{H}$ (which have all the same dimension), and let $U_i:V_i\to V_{i+1}$ be a sequence of unitary operators on $\mathcal{H}$ such that $\sum_{k=1}^\infty\|U_k-\mathbf{1}\|$ exists. Then, the product $\prod_{k=1}^\infty U_k=\ldots\cdot U_3\cdot U_2\cdot U_1$ converges in operator-norm to an isometry $U:V_1\to\mathcal{H}$.

Proof. We first show by induction that $\left\|\prod_{k=1}^N U_k-\mathbf{1}\right\|\leq\sum_{k=1}^N\|U_k-\mathbf{1}\|$. This is trivially true for $N=1$; suppose it is true for N factors, then

$$\begin{aligned}\left\|\prod_{k=1}^{N+1}U_k-\mathbf{1}\right\| &\leq \left\|\prod_{k=1}^{N+1}U_k-\prod_{k=1}^{N}U_k\right\|+\left\|\prod_{k=1}^{N}U_k-\mathbf{1}\right\|\\ &\leq \left\|(U_{N+1}-\mathbf{1})\prod_{k=1}^{N}U_k\right\|+\sum_{k=1}^{N}\|U_k-\mathbf{1}\|\\ &\leq \sum_{k=1}^{N+1}\|U_k-\mathbf{1}\|\ .\end{aligned}$$

By assumption, the sequence $a_n:=\sum_{k=1}^n\|U_k-\mathbf{1}\|$ is a Cauchy sequence; hence, for every $\varepsilon>0$ there is an $N_\varepsilon\in\mathbb{N}$ such that for every $L,N\geq N_\varepsilon$ it holds that $\sum_{k=L+1}^N\|U_k-\mathbf{1}\|<\varepsilon$. Consider now the sequence $V_n:=\prod_{k=1}^n U_k$. If $N\geq L\geq N_\varepsilon$, then

$$\begin{aligned}\|V_N-V_L\| &= \left\|\prod_{k=L+1}^N U_k\cdot\prod_{k=1}^L U_k-\prod_{k=1}^L U_k\right\|\\ &\leq \left\|\prod_{k=L+1}^N U_k-\mathbf{1}\right\|\cdot\left\|\prod_{k=1}^L U_k\right\|\\ &\leq \sum_{k=L+1}^N\|U_k-\mathbf{1}\|<\varepsilon\ ,\end{aligned}$$

so $(V_n)_{n\in\mathbb{N}}$ is also a Cauchy sequence and converges in operator norm to some linear operator U on V_1. It is easily checked that U must be isometric. □

Lemma 1.3 (Norm Inequalities): Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $|\psi\rangle,|\varphi\rangle\in\mathcal{H}$ with $\|\,|\psi\rangle\|=\|\,|\varphi\rangle\|=1$. Then,

$$\|\,|\psi\rangle\langle\psi|-|\varphi\rangle\langle\varphi|\,\|_{\mathrm{Tr}}\leq\|\,|\psi\rangle-|\varphi\rangle\|\ .$$

Moreover, if $\rho,\sigma\in\mathcal{T}_1^+(\mathcal{H})$ are density operators, then

$$\|\rho-\sigma\|\leq\|\rho-\sigma\|_{\mathrm{Tr}}\ .$$

Proof. Let $\Delta := |\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|$. Using [18, 9.99],

$$\begin{aligned}
\|\Delta\|_{\mathrm{Tr}}^2 &= 1 - |\langle\psi|\varphi\rangle|^2 = \left(1 - |\langle\psi|\varphi\rangle|\right)\underbrace{\left(1 + |\langle\psi|\varphi\rangle|\right)}_{\leq 2} \\
&\leq 2 - 2|\langle\psi|\varphi\rangle| \leq 2 - 2\mathrm{Re}\langle\psi|\varphi\rangle \\
&= \langle\psi - \varphi|\psi - \varphi\rangle = \|\,|\psi\rangle - |\varphi\rangle\|^2 \ .
\end{aligned}$$

Let now $\tilde\Delta := \rho - \sigma$, then $\tilde\Delta$ is Hermitian. We may assume that one of its eigenvalues which has largest absolut value is positive (otherwise interchange ρ and σ), thus

$$\begin{aligned}
\|\tilde\Delta\| &= \max_{\|\,|v\rangle\|=1} \langle v|\tilde\Delta|v\rangle = \max_{P \text{ proj., } \mathrm{Tr}P=1} \mathrm{Tr}(P\tilde\Delta) \\
&\leq \max_{P \text{ proj.}} \mathrm{Tr}(P\tilde\Delta) = \|\tilde\Delta\|_{\mathrm{Tr}}
\end{aligned}$$

according to [18, 9.22]. □

Lemma 1.4 (Dimension Bound for Similar Subspaces): Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $V, W \subset \mathcal{H}$ be subspaces such that for every $|v\rangle \in V$ with $\|\,|v\rangle\| = 1$ there is a vector $|w\rangle \in W$ with $\|\,|w\rangle\| = 1$ which satisfies $\|\,|v\rangle - |w\rangle\| \leq \varepsilon$, where $0 < \varepsilon \leq \frac{1}{4(\dim V - 1)^2}$ is fixed. Then, $\dim W \geq \dim V$. Moreover, if additionally $\varepsilon \leq \frac{1}{36}\left(\frac{5}{2}\right)^{2-2\dim V}$ holds, then there exists an isometry $U : V \to W$ such that $\|U - \mathbf{1}\| < \frac{8}{3}\sqrt{\varepsilon}\left(\frac{5}{2}\right)^{\dim V}$.

Proof. Let $\{|v_1\rangle, \ldots, |v_d\rangle\}$ be an orthonormal basis of V. By assumption, there are normalized vectors $\{|w_1\rangle, \ldots, |w_d\rangle\} \subset W$ with $\|\,|v_i\rangle - |w_i\rangle\| \leq \varepsilon$ for every i. From the definition of the trace distance for pure states (see [18, (9.99)] together with Lemma 1.3, it follows for every $i \neq j$

$$\begin{aligned}
\sqrt{1 - |\langle w_i|w_j\rangle|^2} &= \|\,|w_i\rangle\langle w_i| - |w_j\rangle\langle w_j|\,\|_{\mathrm{Tr}} \\
&\geq \|\,|v_i\rangle\langle v_i| - |v_j\rangle\langle v_j|\,\|_{\mathrm{Tr}} \\
&\quad - \|\,|v_i\rangle\langle v_i| - |w_i\rangle\langle w_i|\,\|_{\mathrm{Tr}} \\
&\quad - \|\,|v_j\rangle\langle v_j| - |w_j\rangle\langle w_j|\,\|_{\mathrm{Tr}} \\
&\geq 1 - \|\,|v_i\rangle - |w_i\rangle\| - \|\,|v_j\rangle - |w_j\rangle\| \\
&\geq 1 - 2\varepsilon \ .
\end{aligned}$$

Thus, $|\langle w_i|w_j\rangle| < 2\sqrt{\varepsilon} \leq \frac{1}{d-1}$, and it follows from Lemma 1.1 that $\dim W \geq d$. Now apply the Gram-Schmidt orthonormalization procedure to the vectors $\{|w_i\rangle\}_{i=1}^d$:

$$|\tilde e_k\rangle := |w_k\rangle - \sum_{i=1}^{k-1} \langle w_k|e_i\rangle|e_i\rangle \ , \qquad |e_k\rangle := \frac{|\tilde e_k\rangle}{\|\,|\tilde e_k\rangle\|} \ .$$

Use $\left|\|\,|\tilde e_k\rangle\| - 1\right| = \left|\|\,|\tilde e_k\rangle\| - \|\,|w_k\rangle\|\right| \leq \|\,|\tilde e_k\rangle - |w_k\rangle\|$ and calculate

$$\begin{aligned}
\|\,|\tilde e_k\rangle - |w_k\rangle\| &= \left\| \sum_{i=1}^{k-1} \frac{\langle w_k|\tilde e_i\rangle|\tilde e_i\rangle}{\|\,|\tilde e_i\rangle\|^2} \right\| \\
&\leq \sum_{i=1}^{k-1} \frac{|\langle w_k|\tilde e_i - w_i\rangle| + |\langle w_k|w_i\rangle|}{\|\,|\tilde e_i\rangle\|} \\
&\leq \sum_{i=1}^{k-1} \frac{\|\,|\tilde e_i\rangle - |w_i\rangle\| + 2\sqrt{\varepsilon}}{1 - \|\,|\tilde e_i\rangle - |w_i\rangle\|} \ .
\end{aligned}$$

Let $\Delta_k := \|\,|\tilde e_k\rangle - |w_k\rangle\|$ for every $1 \leq k \leq d$. We will now show by induction that $\Delta_k \leq 2\sqrt{\varepsilon}\left[\frac{2}{5}\left(\frac{5}{2}\right)^k - 1\right]$. This is trivially true for $k = 1$, since $\Delta_1 = 0$. Suppose it is true for every $1 \leq i \leq k-1$, then in particular, $\Delta_i \leq \frac{1}{3}$ by the assumptions on ε given in the statement of this lemma, and

$$\begin{aligned}
\Delta_k &\leq \sum_{i=1}^{k-1} \frac{\Delta_i + 2\sqrt{\varepsilon}}{1 - \Delta_i} \\
&\leq \frac{3}{2}\sum_{i=1}^{k-1}\left(2\sqrt{\varepsilon}\left[\frac{2}{5}\left(\frac{5}{2}\right)^i - 1\right] + 2\sqrt{\varepsilon}\right) \\
&= 2\sqrt{\varepsilon}\left[\frac{2}{5}\left(\frac{5}{2}\right)^k - 1\right] \ .
\end{aligned}$$

Thus, it holds that

$$\begin{aligned}
\|\,|e_k\rangle - |v_k\rangle\| &\leq \|\,|e_k\rangle - |\tilde e_k\rangle\| \\
&\quad + \|\,|\tilde e_k\rangle - |w_k\rangle\| + \|\,|w_k\rangle - |v_k\rangle\| \\
&\leq 2\|\,|\tilde e_k\rangle - |w_k\rangle\| + \varepsilon \\
&\leq 4\sqrt{\varepsilon}\left[\frac{2}{5}\left(\frac{5}{2}\right)^k - 1\right] + \varepsilon \ .
\end{aligned}$$

Now define the linear operator $U : V \to W$ via linear extension of $U|v_i\rangle := |e_i\rangle$ for $1 \leq i \leq d$. This map is an isometry, since it maps an orthonormal basis onto an orthonormal basis of same dimension. By substituting $|v\rangle = \sum_{k=1}^d \alpha_k|v_k\rangle$ and using $\varepsilon < 4\sqrt{\varepsilon}$ and the geometric series, it easily follows that $\|\,U|v\rangle - |v\rangle\| \leq \frac{8}{3}\sqrt{\varepsilon}\left(\frac{5}{2}\right)^d$ if $\|\,|v\rangle\| = 1$. □

Lemma 1.5 (Stability of the Control State): If $|\psi\rangle, |\varphi\rangle, |v\rangle \in \left(\mathbb{C}^2\right)^{\otimes n}$ and $\|\,|\psi\rangle\| = \|\,|\varphi\rangle\| = 1$ and $|v\rangle \neq 0$, then it holds for every QTM M and every $t \in \mathbb{N}_0$

$$\begin{aligned}
&\left|\langle q_f|M_{\mathbf{C}}^t(|\psi\rangle\langle\psi|)|q_f\rangle - \langle q_f|M_{\mathbf{C}}^t(|\varphi\rangle\langle\varphi|)|q_f\rangle\right| \\
&\qquad \leq \left\|\,|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\,\right\|_{\mathrm{Tr}} \ , \\
&\left|\langle q_f|M_{\mathbf{C}}^t(|v\rangle\langle v|)|q_f\rangle - \langle q_f|M_{\mathbf{C}}^t(|v^0\rangle\langle v^0|)|q_f\rangle\right| \\
&\qquad \leq 2 \cdot \left|1 - \|\,|v\rangle\|^2\right| \ .
\end{aligned}$$

Proof. Using the Cauchy-Schwarz inequality, Lemma 1.3 and the contractivity of quantum operations with respect to the trace distance (cf. [18, (9.35)]), we get the chain of inequalities

$$\begin{aligned}
\Delta_t &:= \left|\langle q_f|M_{\mathbf{C}}^t(|\psi\rangle\langle\psi|)|q_f\rangle - \langle q_f|M_{\mathbf{C}}^t(|\varphi\rangle\langle\varphi|)|q_f\rangle\right| \\
&\leq \left\|\,M_{\mathbf{C}}^t\left(|\psi\rangle\langle\psi|\right) - M_{\mathbf{C}}^t\left(|\varphi\rangle\langle\varphi|\right)\right\| \\
&\leq \left\|\,M_{\mathbf{C}}^t\left(|\psi\rangle\langle\psi|\right) - M_{\mathbf{C}}^t\left(|\varphi\rangle\langle\varphi|\right)\right\|_{\mathrm{Tr}} \\
&\leq \left\||\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|\right\|_{\mathrm{Tr}} \ .
\end{aligned}$$

The second inequality can be proved by an analogous calculation, using that $M_{\mathbf{C}}^t(\sigma) = \mathrm{Tr}_{\mathbf{IOH}}\left(V_M^t \sigma V_M^{t\,*}\right)$ and $\|\mathrm{Tr}_B\rho^{AB}\| \leq 2 \cdot \|\rho^{AB}\|$ for density operators ρ^{AB} on a tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, see [20]. □

Acknowledgment

Sincere thanks go to Wim van Dam, Caroline Rogers, Torsten Franz, and David Gross for helpful discussions. Also, the author would like to thank his collegues Ruedi Seiler, Arleta Szkoła, Rainer Siegmund-Schultze, Tyll Krüger, and Fabio Benatti for constant support and encouragement.

REFERENCES

[1] D. Deutsch, ”Quantum theory, the Church-Turing principle and the universal quantum computer”, *Proc. R. Soc. Lond.*, vol. A400, 1985.

[2] R. Feynman, ”Simulating physics with computers”, *International Journal of Theoretical Physics*, vol. 21, pp. 467-488, 1982.

[3] E. Bernstein, U. Vazirani, ”Quantum Complexity Theory”, *SIAM Journal on Computing*, vol. 26, pp. 1411-1473, 1997.

[4] J. Gruska, ”Quantum Computing”, *McGraw–Hill, London*, 1999.

[5] M. Ozawa and H. Nishumura, ”Local Transition Functions of Quantum Turing Machines”, *Theoret. Informatics and Appl.*, vol. 34, pp. 379-402, 2000.

[6] P. Benioff, ”Models of Quantum Turing Machines”, *Fortsch. Phys.*, vol. 46, pp. 423-442, 1998.

[7] J. M. Myers, ”Can a Universal Quantum Computer Be Fully Quantum?”, *Phys. Rev. Lett.*, vol. 78, pp. 18231824, 1997.

[8] N. Linden, S. Popescu, ”The Halting Problem for Quantum Computers”, Preprint, 1998. [Online]. Available: http://arxiv.org/abs/quant-ph/9806054

[9] M. Ozawa, ”Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting”, *Quantum Communication, Computing, and Measurement 2*, pp. 241-248, 2000.

[10] Y. Shi, ”Remarks on Universal Quantum Computer”, *Phys. Lett. A*, vol. 293, pp. 277-282, 2002.

[11] T. Miyadera, M. Ohya, ”On Halting Process of Quantum Turing Machine”, Open Systems and Information Dynamics, vol. 12 Nr. 3, pp. 261-264, 2005.

[12] F. Benatti, T. Krüger, M. Müller, Ra. Siegmund-Schultze, A. Szkoła, ”Entropy and Quantum Kolmogorov Complexity: a Quantum Brudno’s Theorem”, *Commun. Math. Phys.*, vol. 265/2, pp. 437-461, 2006.

[13] M. Li and P. Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer Verlag, 1997.

[14] A. Berthiaume, W. Van Dam and S. Laplante, ”Quantum Kolmogorov complexity”, *J. Comput, System Sci.*, vol. 63, pp. 201-221, 2001.

[15] P. Vitányi, ”Quantum Kolmogorov complexity based on classical descriptions”, *IEEE Trans. Infor. Theory*, vol. 47/6, pp. 2464-2479, 2001.

[16] P. Gács, ”Quantum algorithmic entropy”, *J. Phys. A: Math. Gen.*, vol. 34, pp. 6859-6880, 2001.

[17] C. Rogers, V. Vedral, ”The Second Quantized Quantum Turing Machine and Kolmogorov Complexity”, Preprint, 2005. [Online]. Available: http://arxiv.org/abs/quant-ph/0506266

[18] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[19] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications, John Wiley & Sons, New York, 1991.

[20] V. Paulsen, *Completely Bounded Maps and Operator Algebras*, Cambridge Studies in Advanced Mathematics, 2003.